HP e3000/iX Network Planning and Configuration Guide

HP e3000 MPE/iX Computer Systems

Edition 6

Manufacturing Part Number: 36922-90043
E0801

U.S.A. August 2001

Notice

The information contained in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for direct, indirect, special, incidental or consequential damages in connection with the furnishing or use of this material.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013. Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19 (c) (1,2).

Acknowledgments

Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304 U.S.A.

Contents

Contents

D. PCI 10/100Base-TX/3000 Quick Installation

Figures

Figures

Tables

Tables

Preface

This manual documents functionality for the MPE/iX releases, for HP e3000 systems. It describes the concepts and terminology needed to design an NS 3000/iX network and to plan the configuration process for that network. It also provides step-by-step instructions to assist you in configuring the network links for HP e3000 systems.

Audience

This manual is intended for network managers and planners who are responsible for setting up and configuring a communications network.

To make the best use of this guide, you should be familiar with basic MPE commands as well as with the NS 3000/iX product.

You should also be familiar with NMMGR, the tool used to configure network connections. If not, refer to *Using the Node Management Services (NMS) Utilities* for information.

Special Note

MPE/iX, Multiprogramming Executive with Integrated POSIX, is the latest in a series of forward-compatible operating systems for the HP e3000 line of computers.

In HP documentation and in talking with HP e3000 users, you will encounter references to MPE XL, the direct predecessor of MPE/iX. MPE/iX is a superset of MPE XL. All programs written for MPE XL will run without change under MPE/iX. You can continue to use MPE XL system documentation, although it may not refer to features added to the operating system to support POSIX (for example, hierarchical directories).

Finally, you may encounter references to MPE V, which is the operating system for HP e3000s, not based on the PA_RISC architecture. MPE V software can be run on the PA_RISC HP e3000s in what is known as *compatibility mode*.

Organization

This manual is divided into the following chapters and appendixes:

Chapter 1 , “Network Configuration Overview,” provides information you should know before you begin configuration.

Chapter 2 , “Networking Concepts,” describes networking concepts and provides information you need to know to plan your configuration.

Chapter 3 , “Planning Your Network,” will help you draw your network map and fill out network worksheets as you plan your network, internetwork, gateway, and network directory configuration.

Chapter 4 , “Planning for Node Configuration,” describes how to fill out node worksheets before you start configuring network links for each node. It includes a table listing the parameters that you will need to enter during NMMGR guided configuration.

Chapter 5 , “Introductory Screens,” provides step-by-step instructions for configuring NMMGR introductory screens.

Chapter 6 , “Configuring a LAN Node,” provides step-by-step instructions for configuring IEEE802.3/Ethernet LAN, token ring, and Fiber Distributed Data Interface (FDDI) links.

Chapter 7 , “Configuring a Point-to-Point Node,” provides step-by-step instructions for configuring Point-to-Point (router) links.

Chapter 8 , “Configuring a X.25 Node,” provides step-by-step instructions for configuring X.25 links.

Chapter 9 , “Configuring a Gateway Half,” provides step-by-step instructions for configuring the interface between two gateway halves.

Chapter 10 , “Validating and Cross-Validating with SYSGEN,” provides step-by-step instructions for validating the network transport and cross-validating with SYSGEN.

Chapter 11 , “Configuring the Network Directory,” provides step-by-step instructions for configuring a network directory.

Chapter 12 , “Configuring Domain Name Files,” provides instructions for configuring the domain name resolver.

Chapter 13 , “Configuring Logging,” provides step-by-step instructions for configuring logging.

Chapter 14 , “Operating the Network,” shows you how to bring up and shut down NS 3000 links and services.

Appendix A , “MPE/V to MPE/iX Migration,” provides general MPE/V to MPE/iX migration information.

Appendix B , “NS X.25 Migration: NS 3000/V to NS 3000/iX,” provides X.25-specific information on migration from a node running NS X.25 3000/V Link to a node that will be running NS 3000/iX release 2.0 or later. Appendix C does not apply if an MPE V-based node s being used as an X.25 server for NS 3000/XL-based machines.

Appendix C , “NS X.25 Migration: NS 3000/V PAD Access to NS 3000/iX,” tells how to migrate NS 3000/V versions of PAD access to NS 3000/iX release 2.0 or later.

Glossary, contains terms applicable to the network configuration process.

Related HP Publications

The following manuals are referenced in this manual or may be of use to you as you plan and configure your network.

Networking

- *Using the Node Management Services (NMS) Utilities*
- *Configuring and Managing Host-Based X.25 Links*
- *Managing Host-Based X.25 Links Quick Reference Guide*
- *NS 3000/iX NMMGR Screens Reference Manual*
- *NS 3000/iX Operations and Maintenance Reference Manual*
- *NS 3000/iX Error Messages Reference Manual*
- *NetIPC 3000/XL Programmer's Reference Manua*l
- *Berkeley Sockets/iX Reference Manual*
- *Using NS 3000/iX Network Services*

Datacommunications and Terminal Subsystem

Configuring Systems for Terminals, Printers, and Other Serial Devices and *Troubleshooting Terminal, Printer, and Serial Device Connections*

Using the OpenView DTC Manager

General Information

System Startup, Configuration, and Shutdown Reference Manual

MPE/iX Commands Reference Manual

Hardware Installation Guides

- *PCI 100Base-T Network Adapter Installation and Service Guide*
- *HP-PB 100Base-T Network Adapter Installation and Service Guide*
- *8-Port Serial PCI ACC Multiplexer Installation and User's Guide*
- *HP-PB 100VG-AnyLAN Network Adapter Installation and Service Guide*
- *HP-IB FDDI Adapter Installation Guide*

1 Network Configuration Overview

This manual provides step-by-step instructions you can use to configure an HP e3000 node for network communications. You can use the information to configure an IEEE 802.3/Ethernet, Token Ring, FDDI, 100VG-AnyLAN, 100Base-T, Point-to-Point (router), or X.25 node.

Before you begin configuration, you must ensure your network is physically set up and ready for network configuration.

This chapter provides information you should know before you begin configuration. It tells you what preparations you must make and what items you will be configuring.

This chapter contains the following configuration information:

- Pre-configuration hardware check.
- Pre-configuration software check.
- Configuration process overview.

Pre-Configuration Hardware Check

Before beginning the actual configuration process, check that the hardware components required for NS 3000/iX have been installed and verified according to the procedures in the hardware installation manuals listed in the preface to this guide.

Pre-Configuration Software Check

Once you have verified that your hardware has been correctly installed, verify that the appropriate software is installed by performing the following steps:

1. Ensure that the Datacommunications and Terminal Subsystem (DTS) has been configured. If DTS has not been configured, refer to *Configuring Systems for Terminals, Printers, and Other Serial Devices* and configure the DTS before proceeding.
2. Check that the data communications software has been installed properly by running the NMMAINT program (`NMMAINT.PUB.SYS`), which is supplied as part of the node management services. NMMAINT will tell you if any software modules are missing or invalid. See the *Using the Node Management Services (NMS) Utilities* manual for a discussion of the NMMAINT program.
3. Whenever you receive a new version of the node management services (NMS) software (which includes NMMGR), and you have earlier versions of NMS, you first have to run a conversion program. The conversion program, called NMMGRVER (`NMMGRVER.PUB.SYS`), ensures that configuration files created with an earlier version of NMMGR are converted to the latest format.

Configuration Process Overview

The instructions in this guide explain how to configure each node on your network by using a "guided" branch of Hewlett-Packard's NMMGR configuration program. The principal steps in this process are as follows:

1. Plan your network before you begin NMMGR. Use the worksheets provided in Chapter 4 , "Planning for Node Configuration," to record all the items NMMGR requires. (See Chapter 2 , "Networking Concepts," for information on networking concepts.)
2. Configure the transport and link by using NMMGR to modify the `NMCONFIG.PUB.SYS` file. The instructions for this step are contained in this manual.
3. If the node being configured is part of an internet or is on a network with non-HP nodes, add the path of the new node to its network directory file. See Chapter 11 , "Configuring the Network Directory," for information on configuring the network directory, or if using DNS for nodename resolution.
4. Validate the network transport. This step checks data consistency between values entered on different NMMGR data entry screens. Instructions for validating the network transport are located in Chapter 10 , "Validating and Cross-Validating with SYSGEN."
5. Cross-validate `NMCONFIG.PUB.SYS` with the system configuration files within SYSGEN. Cross-validation ensures that there are no conflicts in the use of node names, device classes, and physical paths. Even if validation and cross-validation were already done after configuring DTS, you still have to validate and cross-validate again after you configure the network transport and link. Instructions for cross-validating are located in Chapter 10 , "Validating and Cross-Validating with SYSGEN."
6. Start the network (links and services) using the `NETCONTROL` and `NSCONTROL` commands. See Chapter 14 , "Operating the Network," for information on starting links and services.
7. Verify the NS services configuration and confirm network connectivity by running the `QVALNS` program. See Chapter 14 , "Operating the Network," for information on running `QVALNS`.

2 Networking Concepts

Planning a network or internetwork (collection of networks) is an important process that must be done with care to ensure that the network meets the needs of your organization. Many factors must be taken into consideration when planning the network or internetwork: for example, volume of usage over particular links, volume of CPU usage of each node, physical layout needs and limitations (such as geographical distances), and desirability of connections to non-NS 3000/iX nodes.

This chapter provides information to help you design your network and plan for configuration using NMMGR. The following network design elements are discussed:

- Design considerations of the network environment
- Network interface and link types
- Subnetworks
- Internetworks
- Address resolution methods:
  - — Domain names
  - — Network directory
  - — Probe and probe proxy
  - — Address Resolution Protocol (ARP)

Network Environment Design Considerations

Network and internetwork design must take many factors into consideration: the desired physical location of the computers comprising the network, the volume of projected communications traffic between nodes, communications traffic patterns, and the possibility of connections to other types of nodes (such as those in a public data network) are just some of the criteria to consider.

These factors will affect your choice of NS network type (LAN, Token Ring, FDDI, 100VG-AnyLAN, 100Base-T, Point-to-Point, X.25) as well as choice of specific links. They will also affect how you design your network layout. You may want to create subnetworks within your network by configuring IP subnet addresses. You may, on the other hand, need to join several networks together to form an **internetwork** or **internet**.

Line Speed

Line Speed is a measure of the rate at which data is transmitted by a physical link (usually measured in kilobits or megabits per second). The maximum line speed varies among different NS links. Line speed may therefore influence your choice of link. Although line speed does not indicate the exact throughput of a particular link, it can be used on a comparative basis to indicate relative throughput.

In general, an IEEE 802.3/Ethernet LAN or Token Ring network will be faster than a Point-to-Point or X.25 network because the bus or ring topology provides a faster routing mechanism than a series of Point-to-Point hops. FDDI, 100VG-AnyLAN, and 100Base-T links will be an order of magnitude faster than LAN or Token Ring. Links using leased lines will have a higher line speed than links using normal telephone lines.

Consult your Hewlett-Packard representative for line speeds and the most up-to-date performance data for various links.

Geographical Location

The geographical location of the computers that will be part of your network or internet will be an important factor in deciding both the physical topology and the link types that you should use.

If all of the nodes you want to connect are located relatively close to each other (in the same building, for example) you might choose to connect them via a LAN, Token Ring link, 100VG-AnyLAN, or 100Base-T.

Another option for nodes located in the same geographic location is to use hardwired (direct-connect) Point-to-Point links. You might wish to

use a Point-to-Point network if the distance between some nodes on the network will be greater than the maximum distance allowed between nodes on a LAN. Bridges, hubs and routers are commonly implemented to extend LANs.

FDDI networks also offer greater distances than LAN, Token Ring, 100VG-AnyLAN, or 100Base-T networks. FDDI networks can be up to 200 kilometers in length, with nodes up to 2 kilometers apart.

If you need to connect nodes that are geographically distant (for example, HP e3000s located in different cities) you might choose to connect them via a dial link. For NS dial links, you can use the Point-to-Point 3000/iX Network Link.

Finally, if you need to use satellite transmission because of the large geographical distance between nodes, or if you need to have access to other nodes on a public or private X.25 network, you might wish to use the DTC/X.25 iX Network Link.

Special Cases

The following sections describe certain design requirements for special situations, such as shared dial links, personal computers, and using non-HP e3000 minicomputers on an NS network.

Shared Dial Links

Shared dial links have two limitations that must be considered when designing a network. First, a shared dial link cannot be used as an intermediate link in a Point-to-Point network. Any other kind of dial link can be used for intermediate links, but shared dial links can be used only to connect leaf nodes (that is, nodes that receive messages targeted only for themselves, also referred to as end nodes). Second, cannot dial out on SMUX, shared dial links cannot be used as gateway halves.

Non-HP e3000 Nodes (Including PCs)

LAN, Token Ring, FDDI, 100VG-AnyLAN, 100Base-T, and X.25 networks can access non-HP e3000 nodes. Point-to-Point networks must be composed of only HP e3000s.

Applicable SYSGEN Parameters

VT terminals are not physical devices, instead they are virtual devices created dynamically at remote logon, header entries are created for the maximum number of VT terminals at system boot time. The exact number of head entries created for VT terminals will depend on the value of MAXDYNIO (which is configurable in SYSGEN).

The exact number of remote sessions which can be supported on a given system will depend on the exact mix of jobs and sessions (remote and local, active and inactive) on that system.

The maximum number of concurrent processes may limit the number of remote logons before the maximum number of dynamic I/O devices does.

Dynamic Ldevs

This is actually a system parameter that can be configured to 999 in SYSGEN. The default is 332, but the actual number that can be in use may be limited by the IDD/ODD limits. VT and NS use one dynamic ldev per remote session and one per LAN link and one per Point-to-Point link.

NOTE

The result of having DYNAMIC IO DEVS configured too low for NS VIRTUAL TERMINAL connections is VTERR 8 or VT INFORM 050.

Likewise the dynamic I/O device limit may be reached before the concurrent process limit.

Network Interface and Link Types

The network interface (NI), the software that provides an interface between a node and a network, specifies the type and maximum number of links that can be configured for a node. Because a node's network interface determines what links can be configured for the node, links are said to be configured underneath network interfaces.

There are nine types of network interfaces (in addition to loopback):

- **LAN** for IEEE 802.3 and Ethernet networks, 100VG-AnyLAN networks, and 100Base-T networks.
- **Token Ring** for IEEE 802.5 networks.
- **FDDI** for fiber optic networks.
- **100VG-AnyLAN** for 100VG-AnyLAN networks.
- **100Base-T** for 100Base-T networks.
- **Point-to-Point** for networks that use Point-to-Point routing.
- **X.25** for X.25 networks.
- **NS over SNA** is no longer offered as a product and has been removed from the Corporate Price List. The product is obsolete with no plans for support.
- **Gateway half** for nodes that function as gateway halves.

Number of Network Interfaces

A system can have up to 48 network interfaces (NI) configured. One of these network interfaces must be loopback. For each network interface, the maximum number of links you can configure and the kinds of links possible are determined by the network interface type, as follows:

- A LAN network interface can have only one link configured under it; however, a single link can reach a large number of nodes. ThickLAN cable supports up to 100 nodes per segment; ThinLAN cable can be used for up to 30 nodes per segment; and each Ethertwist 3000/iX can be used for up to 50 nodes. **Up to two LAN NIs can be active at a time per system, 100BT allows a maximum distance of 100m between 2 nodes.**
- A Token Ring interface can have only one link configured under it; however, a single link can reach a large number of nodes. Token Ring 3000/iX Network Link can support up to 250 nodes per ring using shielded twisted pair (STP) cabling at 4 or 16 Mbps and 50 nodes per ring using unshielded twisted pair (UTP) cabling at 4 Mbps. **Only one Token Ring NI can be active at a time per system.**

- An FDDI interface can have only one link configured under it; however, a single link can reach a large number of nodes. FDDI/iX Network Link can support up to 1000 nodes. **Up to four FDDI NIs can be active at a time per system**.
- A Point-to-Point network interface can have up to 40 links configured under it. Point-to-Point links may be dial links, in which a modem attached to a node is used to transmit and receive data carried across telephone wires, or leased lines, in which data is sent over data-grade lines leased from a private carrier. **Up to 11 Point-to-Point NI's can be active at a time (one NI must be loopback) for a total of 12 NI's per system.**.
- An X.25 network interface can have from one to 11 links configured, depending on the number of configured X.25 network interfaces on the node. (A single node can have up to 11 NIs and up to 11 X.25 links.) Each link can be connected to as many as 1,024 remote nodes, with communication allowed with as many as 256 nodes at the same time. **Up to 11 X.25 NI's can be active at a time (one NI must be loopback) for a total of 12 NI's per system.**.
- A gateway half network interface can have only one link configured under it (the gateway half link). Links connecting two gateway halves can be only NS Point-to-Point 3000/iX Network links. **Only one gateway half NI can be active at a time per system**.

If more than one (non-loopback) network interface is configured on a node, the network portions of the IP addresses configured for the interfaces should differ to correspond to the multiple networks to which the node belongs.

Refer to "Software Configuration Maximums" at the end of this chapter for information on configuration path maximums.

Priority of Network Interfaces

If it is possible to reach a destination through more than one active NI, the network determines which NI to select according to the following priority:

Loopback
100VG-AnyLAN
100Base-T
FDDI
LAN
Token Ring
X.25
Gateway Half
Point-to-Point (router)

If more than one NI of a given type is active, (for example, two X.25 NIs) the network will select the one that it finds first.

Subnetworks

IP Subnets are used to divide one network into two or more distinct subnetworks. Subnet numbers identify subnetworks in the same way that network addresses identify physically distinct networks. Subnetting divides the node address portion of an IP address into two portions—one for identifying a specific subnetwork and one for identifying a node on that subnetwork.

Why Use Subnets?

The use of subnets is optional. Subnets are typically used in organizations that have a large number of computers. You may want two or more physically distinct networks to share the same network address. This may occur, for example, if your organization has acquired only one network number, but any of the following is true:

- A few nodes on a single network create the bulk of the network traffic and you want to isolate those nodes on a subnetwork to reduce overall congestion.
- You have a single LAN and have reached the limit of its technology in terms of node numbers or cable length.
- LANs are located too far apart to be joined with bridges.

How Subnetting Works

You may use subnets to divide your current network into subnetworks without informing remote networks about an internal change in connectivity. A packet will be routed to the proper subnet when it arrives at the gateway node. However, if you want a remote node to know about only some of the subnets on your network, this must be configured.

The network portion of an IP address must be the same for each subnetwork of the same network. The subnet portion of an IP address must be the same for each node on the same subnetwork.

Assigning Subnet Masks

Before you can determine subnet numbers, you first must determine which bits of the node address will be used to contain your subnet numbers.

The bits that you designate for subnet identifiers compose the subnet mask. The subnet mask is configured with NMMGR. The remaining part of the node address is used to identify the host portion of the IP address.

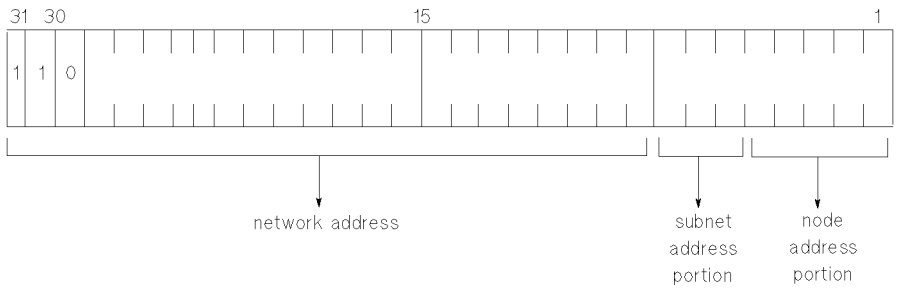
The following rules apply when choosing a subnet mask and an IP address:

- Although any bits in the node address can be used as the subnet mask, Hewlett-Packard recommends aligning the subnet mask along byte boundaries, adjacent to the network number.
- Although standards allow subnets on the same network to have different subnet masks, Hewlett-Packard recommends that you assign the same subnet mask to all subnets on a network.
- Do not assign an IP address where the network address and/or node address bits are all off (all 0s) or all on (all 1s). Likewise, the subnet address bits cannot be all 0s or all 1s.

To determine the subnet mask, you first need to estimate the number of networks required and the number of nodes on each subnet. Allow enough bits for both nodes and subnets, as described in example 1.

Example 1 Assume you are choosing a subnet mask for a class C network (three bytes for network address, one byte for node address), and you need four subnets with up to 30 nodes on each subnet. You will need to reserve three bits for the subnet address (remember, all 0s and all 1s cannot be used) and the remaining five bits for the node numbers as shown in Figure 2-1.

Figure 2-1 Class C Address with Subnet Number

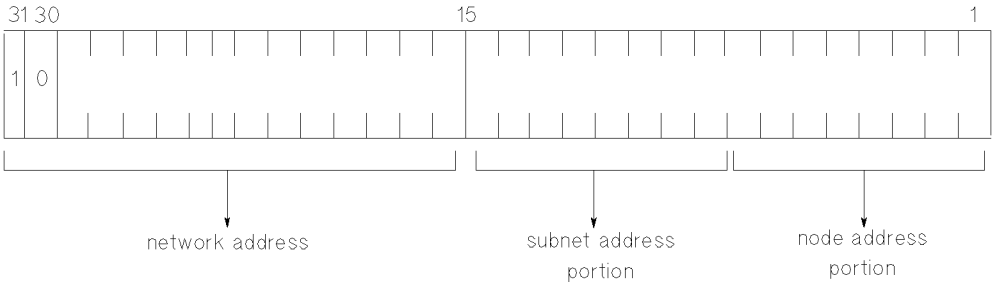


The 30 nodes per subnet will require at least five bits of the node portion of the IP address (30 <32, and $32=2^5$, therefore you need 5 bits). This leaves three bits remaining in the node portion of the IP address for use as the subnet identifier. Subnet parts of all 0's or all 1's are not recommended because they can be confused with broadcast addresses.

Therefore, you can have up to six subnets ($2^3 -2=6$) when three bits are used for the subnet identifier.

Example 2 An IP address on a class B network with an 8-bit subnet mask separates as shown in Figure 2-2.

Figure 2-2 Class C Address with Subnet Number



Now, refer again to example 1. The subnet mask must indicate that three bits of the node portion of the IP address will be used for the subnet identifier. The subnet mask turns on (sets to 1) all the relevant bits for its subnet scheme. The subnet mask for example 1 is shown below. Note that the most significant three bits of the rightmost byte are set.

Subnet Mask

Binary `11111111.11111111.11111111 11100000`

Decimal `255.255.255 224`

Table 2-1 shows valid addresses for the subnetwork in example 1. You will need to know this information for NMMGR configuration. The table shows the possible values of the rightmost byte of the IP address for each of the subnets, given the criteria described in the example. (Remember, an address of all 0s or all 1s is not valid).

Column 2 shows the values, in binary, of the six subnet addresses. Five zeroes are shown in parentheses to indicate where the three subnet-address bits are located in the byte. The equivalent decimal value for each subnet address is shown in the third column. The fourth column shows the range of possible values for the node address of each subnet. The five rightmost bits make up the node portion, and the range is the same for all subnets. By combining the subnet address with the range of node addresses, the possible decimal values of the rightmost byte are obtained and shown in the fifth column.

The table shows that subnets of 30 nodes each are possible given a subnet mask of `255.255.255 224`. This is derived from the column that shows the range of possible values for the five bits that make up the node portion of the IP address. The range for each of the six subnets shows 30 possible values.

Table 2-1 Valid Addresses of Example Subnetwork

Subnet	Address of Subnetwork in Binary	Decimal Value of Subnetwork	Possible Node Address on Subnetwork	Decimal Value of Rightmost Byte
1	001 (00000)	32	00001–11110	33–62
2	010 (00000)	64	00001–11110	65–94
3	011 (00000)	96	00001–11110	97–126
4	100 (00000)	128	00001–11110	129–158
5	101 (00000)	160	00001–11110	161–190
6	110 (00000)	192	00001–11110	193–222

By looking at the binary values of two IP addresses, it is easy to tell if nodes belong to the same subnet. If they do, all the bits that make up the subnet mask will be the same between IP addresses in the subnet.

Take, for example, two IP addresses (in decimal and in binary) of subnet number 1 from Table 2-1:

```
192.6.12.41  1100 0000 0000 0110 0000 1100 0010 1001
```

```
192.6.12.55  1100 0000 0000 0110 0000 1100 0011 0111
```

The subnet mask has already been defined as:

```
255.255.255 224 1111 1111 1111 1111 1111 1111 1110 0000
```

Because the mask has all bits except the five rightmost bits set to 1, all bits except the five rightmost bits must match between nodes on the same subnet. Because the two example IP addresses from subnet 1 do match except for their five rightmost bits, they belong to the same subnet.

NOTE Subnet addressing can be used in internetworks (networks with gateways).

Internetworks

Two or more networks of the same type or of different types can be linked together to form an internetwork or internet. For example, if you wanted to connect the nodes in a Point-to-Point network with the nodes on a LAN, the combination of the two networks would be called an internetwork. Creation of an internetwork allows any node on one network to communicate with any node on another network that is part of the same internetwork. Up to 256 individual networks can belong to the same NS internetwork.

The divisions between the networks in an internetwork are called network boundaries. Nodes in each network will have the same network address (network portion of the IP address); however, each network within the internetwork will have its own unique network address.

The networks in an internetwork may be connected by a bridge or router, or by HP e3000 systems configured as gateways.

Gateways

One method of joining networks in an internetwork is by using gateways. An HP e3000 system can have up to 256 gateways (combined number of full gateways and gateway halves).

Full Gateways versus Gateway Halves

NS 3000/iX allows you to choose between connecting two networks with a full gateway or connecting them with two gateway halves. A full gateway is a node configured as a full member of two (or more) networks for the purpose of passing information between the networks to which it belongs. The node is considered a member of each of the networks for which it is configured.

A node that is a gateway half is configured as a member of a network and as a partner of another gateway half. A gateway half link that joins two networks connects two nodes (a gateway half pair) by a Point-to-Point link (NS Point-to-Point 3000/iX Network link). The gateway half link and pair is not considered a network itself. Each of the paired gateway halves is configured as a member of a different network (the two networks to be connected) and as a gateway half on the same gateway half link. Together, the two gateway halves function as a full gateway.

Gateway Configuration Overview

Gateway configuration includes both identifying neighbor gateways in each node's configuration file and configuring gateway half NIs for nodes that will serve as one half of a gateway half pair. These tasks are described as follows.

Identifying Neighbor Gateways

If you are including gateways in your internet configuration, you may want to modify each node's configuration file so that the node is aware of all of its neighbor gateways (gateways on the same link). You accomplish this during configuration of each network interface for which you want to allow communications over the gateway. You will find step-by-step instructions for identifying neighbor gateways in each of the link configuration sections of this manual.

An alternative to identifying neighbor gateways in every node's configuration file is to configure a default gateway for the node. Instructions for doing so are included in this manual.

The next pages show several examples of gateway configuration.

Neighbor Gateway Examples

When using NMMGR to configure any node, you will be entering the identities of all the neighbor gateways into the configuration of the node. The following examples illustrate several gateway configuration scenarios based on the network represented in Figure 2-3.

- **Example 1**: The node you are configuring may be a non-gateway, such as node D in Figure 2-3. You would need to enter the identities of each of its neighbor gateways, in this case nodes C and E, at the Neighbor Gateways screen. On the Neighbor Gateway Reachable Networks screen, you would also enter the IP addresses of networks 1 and 3 as two of the configured reachable networks reachable through gateway node C.
- **Example 2**: The node you are configuring may be a gateway half, such as node E in Figure 2-3. You will still need to enter the identities of the node's neighbor gateways as you configure the NI (in this case, node C is the neighbor gateway). You will also need to configure a gateway half NI for the node, as described under "Configuring a Gateway-Half Pair."
- **Example 3**: The node you are configuring may be a full gateway, such as nodes B and C in Figure 2-3. Though full gateways are never actually identified as such in the configuration process, they too, must know about the other gateways. If you were configuring node C, you would identify nodes B and E and neighbor gateways.

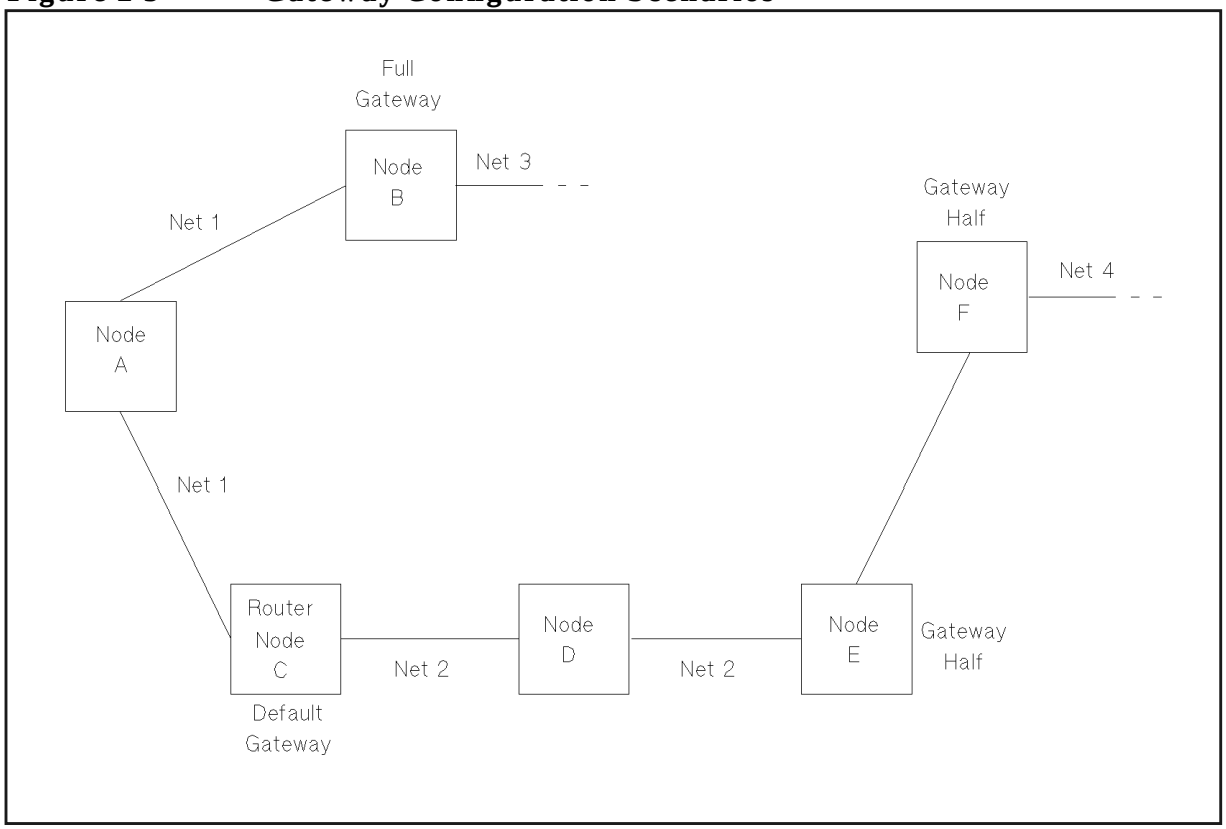
- **Example 4**: One of the gateways on your internetwork may be designated as a default gateway, such as node C in Figure 2-3. A default gateway is a gateway that is designated to receive any traffic for which the network is unable to identify a destination. You must identify the node as a default gateway in the configuration file of each node that will access it as the default gateway. If you were configuring node D, you would identify node C as a default gateway by entering an at sign (@) in one of the IP address fields of the Neighbor Gateway Reachable Networks screen. Only one gateway may be designated as a default gateway for each node. The default gateway must be on a LAN or Token Ring network.

Configuring a Gateway Half Pair

If you are configuring a gateway half pair, you will need to configure a gateway half NI for each half of the gateway pair. You will find step-by-step instructions for configuring a gateway half NI in this manual.

In Figure 2-3, nodes E and F form a gateway half pair. When you configure a node as a gateway half, you enter its partner's IP address into this gateway half's configuration in the Gatehalf Configuration screen. If you were to configure node E in the figure, you would enter the IP address of node F.

Figure 2-3 Gateway Configuration Scenarios



Gateway halves require the configuration of two separate network interfaces on each node: one for the gateway half, the other for the network it interfaces to (for example, a LAN or Point-to-Point NI). You will need to follow the instructions for the specific NI type, depending on the network type) and then follow the instructions to enter configuration items specific to the gateway half NI.

Worksheets that will aid you in planning for internetwork communication are located in Chapter 4 , “Planning for Node Configuration.”

Address Resolution

Address resolution in NS networks refers to the mapping of node names to IP addresses and the mapping of IP addresses to lower level addresses (such as an X.25 address or a station address). Several address resolution methods are available for you to use individually or in combination with each other. You can configure these methods according to the needs of your network.

The available address resolution methods are:

- Domain name services.
- Network directory.
- Probe (and probe proxy) (LAN, 100VG-AnyLAN, and 100Base-T only).
- Address resolution protocol (ARP) (LAN, Token Ring, FDDI, 100VG-AnyLAN, and 100Base-T only).

Domain Name Services

The domain name services are a mechanism for resolving node names to IP addresses. They conform to an open networking standard and will facilitate communications between HP e3000 systems as well as with non-HP e3000 nodes.

To use the domain name services, you must assign a name, in ARPANET standard format, to each system on the network or internetwork. You configure this name on the NS Configuration screen (see configuration chapters for details).

You will also need to create a set of ASCII files on each system which contain the addressing information the system will need. Instructions for creating these files are in Chapter 12 , “Configuring Domain Name Files.”

Once you have configured the domain name services, the network will be able to access the node using its domain name and the domain name service routines will resolve the domain name to the node’s IP address.

NOTE Domain name services provide name to IP address resolution only. If a lower level address is required for network communication (for example, an X.25 address) you will need to configure the network directory as well.

Network Directory

The network directory is a set of files that contain information used by the node to communicate with other nodes in the internetwork.

You use NMMGR to perform the following network directory functions:

- Add, modify, and delete entries in the directory.
- Review and inspect directory information.
- Merge a remote directory with a directory on the local node.
- Automatically update directories on a group of remote nodes by using a background stream job controlled from a central administrative node.

See Chapter 11 , “Configuring the Network Directory,” for more information on configuring the network directory through NMMGR. More information on merging directories and on central administrative nodes is included in this chapter.

When a Network Directory is Required

A network directory must be configured in the following circumstances:

- nodes running on X.25
- nodes not using domain name services
- nodes on a LAN network that do not support the HP-PROBE protocol

The network directory of a node in a Point-to-Point network must contain the IP addresses of all other nodes that you want the node to be able to reach.

When configuring the network directory for a Point-to-Point network, make sure that the IP address you enter in the network directory matches the data in the mapping screens (path name `NETXPORT.NI.`*`NIname`*`.MAPPING.mapentry`).

For nodes on an X.25 network, the network directory maps the X.25 address key to an IP address to allow a node to communicate within the X.25 network. You must configure a network directory for nodes using X.25.

Planning the Network Directory

There are two theories about how network directories should be planned and configured on a network, as follows:

- Centralized network directories.
- Decentralized network directories.

The centralized theory requires each node on the internet to have the same network directory. This means that every node in the network must have an entry in the network directory. The advantage to this is that you update the network directory in one place, then copy it to the rest of the world. The disadvantage is that network directories for large internets are going to be large.

The recommended way to create and maintain your network directory using the centralized method is to assign a single node as the central administrative node. You configure the network directory on this node and then copy it to all other nodes on the network. When the network directory is updated, it is updated on the central administrative node, then copied to the other nodes. This procedure decreases the possibility of incompatible directories. You may want to assign a central administrative node for each network or for the entire internet.

The decentralized theory suggests that each network directory be configured individually on each node. The advantage to this is that you can customize the network directory on each node for security purposes using local and global entries. The network directory will also be smaller because it will only contain entries for that particular node. However, updates must be done manually on each node.

Copying and Merging Network Directory Files

The first time you configure the network directory, an entry for all remote IP addresses must be added manually using the NMMGR screens. After the first network directory is configured, you can use the MPE `STORE` and `RESTORE` commands to copy the network directory to other nodes. (This is assuming you have adopted the centralized method of network directory maintenance. If you use the decentralized method, you must always use NMMGR to create and maintain the network directory.)

NOTE The network directory uses a KSAM file pair. Therefore, when copying a directory, be sure to copy both the data file and the key file. The system names the key file automatically using the first six letters of the network directory file name appended with a K. For example, `NSDIRK.NET.SYS` is the name of the key file associated with the data file `NSDIR.NET.SYS`.

Once a network directory has been established on each node in the internet, you can set up a job stream to automate network directory updates. The `MERGEDIR` command is part of a maintenance interface provided primarily to support the updating of directories using a batch job. Using this method, a job or series of jobs can be scheduled at regular intervals to copy and then merge remote directories into the local-system directory. See the `MERGEDIR` and the `MAKESTREAM` commands in *Using the Node Management Services (NMS) Utilities*.

Probe and Probe Proxy

NS 3000 LAN, 100VG-AnyLAN, and 100Base-T NIs with the IEEE 802.3 protocol enabled are able to make use of a proprietary HP protocol called **probe**. Probe makes it possible for nodes on an NS IEEE 802.3 LAN, 100VG-AnyLAN, and 100Base-T to communicate without a network directory or domain names. A node can determine connection information about a node on the same LAN by sending a multicast probe request out on the network. The target node recognizes its address in the probe request and sends an individually addressed probe reply with the necessary connection information to the requesting node. The probe request/reply mechanism is sufficient to obtain connection requirements within a network.

If the nodes on that LAN are to communicate with other networks, at least one node on the network must have a network directory. The node with the network directory is called a **proxy server**. By using the probe protocol, a node without a network directory can multicast a request for an internet address from the proxy server. For backup purposes, you should designate at least two nodes to be proxy servers.

Address Resolution Protocol (ARP)

HP e3000 LAN, Token Ring, FDDI, 100VG-AnyLAN, AND 100Base-T NIs are able to make use of a standard protocol called Address Resolution Protocol (ARP). ARP provides IP address to station address resolution. ARP is enabled when the Ethernet protocol or Token Ring is enabled.

Enabling Probe and ARP

With the concurrent configuration of IEEE 802.3 and Ethernet on a network, both the probe and ARP protocols are also enabled. Both protocols broadcast requests to all nodes on the network to resolve the address of a given remote node.

If you disable IEEE 802.3 on a LAN NI, you also disable the probe protocol. Likewise, by disabling Ethernet, you disable the ARP protocol associated with it. You cannot disable both of these protocols simultaneously; at least one must be active to facilitate network communications.

Network Design Questions

Ask yourself the following questions to make sure your design adheres to the considerations mentioned above:

1. Are all of the nodes in the network within roughly 200 meters of each other?

   If so, consider connecting them with 100Base-T links, or ThinLAN links with Ethertwist. For entry-level servers, choose ThinLAN since that adapter will offload part of the CPU load.

2. Are all of the nodes in the network within roughly 550 meters of each other?

   If so, consider connecting them with ThinLAN 3000/iX links. The maximum cable length for segments of ThinLAN 3000/iX cable is 185 meters, with a maximum of three segments connected by repeaters.

3. Are all of the nodes in the network within roughly 1,500 meters of each other?

   If so, consider connecting them with ThickLAN (thick coaxial cable). The maximum cable length for each segment of ThickLAN coaxial cable is 500 meters, with a maximum of three segments connected by repeaters.

4. Are all of the nodes in the network located within 2 kilometers of each other?

   If so, consider using FDDI/iX links. The maximum cable length for each segment is 2 kilometers with a maximum network length of up to 200 kilometers.

5. Are nodes located at remote sites? (For example, in different buildings in the same city, or in different cities?)

   If so, consider installing an X.25 network or a Point-to-Point network using dial links or leased lines. Choose leased lines if you have a critical need for clear transmission or if the volume of data to be transmitted is relatively large.

   Routers, switches, bridges and hubs are used to set up networks.

   - Routers are used to route packets between networks and subnets based on the packets destination address.
   - Bridges are used to connect two LAN networks that are far apart.
   - Hubs are multiport repeaters, used to build or extend a LAN network. New nodes can be added to the LAN without disrupting the existing network.

- To connect two networks that run on different protocol stacks, a gateway is needed. A gateway does conversion between the two protocols at every layer until the application layer.

6. Is the set of nodes you wish to connect composed of some nodes that are in close proximity to one another (for example, in the same building) and other nodes that are geographically distanced (for example, in different buildings or different cities)?

   If so, you may wish to use ThinLAN 3000/iX, Token Ring 3000/iX, FDDI, 100VG-AnyLAN, or 100Base-T networks for nodes that are located near one another and Point-to-Point or X.25 links for nodes in different buildings or cities.

7. Will HP 9000s or other minicomputers need to be part of the network?

   If so, consider ThinLAN 3000/iX (or its ThickLAN option), Token Ring 3000/iX, FDDI/iX, 100VG-AnyLAN, 100Base-T, or X.25/iX System Access.

8. Do you need access to nodes on public or private X.25 networks?

   If so, consider using DTC/X.25 iX Network Links.

9. Is a subset of nodes either geographically or organizationally distanced from another subset of nodes?

   If so, you may wish to establish a network boundary between them in order to make them two separate networks joined by a full gateway or router. Alternatively, you may want to use subnets to divide one network into two or more physically distinct subnetworks.

10. If you must use a gateway half, is the partner-gateway half in the same building or further away?

    If the two gateway halves are in the same building, you can use a direct connect link between them. If the two gateway halves are further away, you will need to use a dial link.

Software Configuration Maximums

The software maximums as shown in Table 2-2, must be adhered to when configuring a supported link. These maximums may be further limited by the system hardware (number of available slots). Maximums are also documented throughout the manual for the appropriate screen.

Table 2-2 Configuration Maximums

NMMGR Screen Number/Description	Path	Maximum Limit
#9 Network Directory Select Node Name	None	File Size Limit
#44 Point-to-Point Link Configuration	None	40 links/Router NI (8 per screen)
#45 Direct Connect/Dial Node Mapping Configuration	None	1024 Mappings/Router
#46 Shared Dial Node Mapping Configuration	None	1024 Mappings/Router
#48 X.25 Configuration	None	11 Links/X.25 NI
#112 Network Interface Configuration	NETXPORT.NI	48 NI/system
#117 Gateway Half NI Links	NETXPORT.NI.*NIname*.LINK	1 link/Gateway Half NI
#158 Neighbor Gateway Reachable Networks	NETXPORT.NI.*NIname*.INTERNET.gatewayn	2550 networks/NI
#85 Link Selection	LINK	256 Links/System

3 Planning Your Network

This chapter will help you to draw your network map and contains worksheets to help you plan your network, internetwork, gateway, and network directory configuration. You will need to consider a number of items as you plan your configuration. This chapter provides guidelines to help you accomplish the following:

- Draw an internetwork map.
- Complete the internetwork table.
- Draw a network map and complete network worksheets for each link that you are configuring.
- Complete the network directory worksheet if a network directory is required.
- Update Domain name files if using DNS for node name resolution. Refer to Chapter 12 , “Configuring Domain Name Files.”

Drawing an Internetwork Map

This section deals with the internetwork as a whole. The internetwork worksheets consist of an internetwork map, which shows an overview of your internetwork, and an internetwork table. You will take the following steps when filling out the internetwork worksheets:

- Draw sketches of each network in the internetwork.
- Write network names, IP network addresses, and network types.
- Draw gateway nodes.
- Indicate network boundaries.

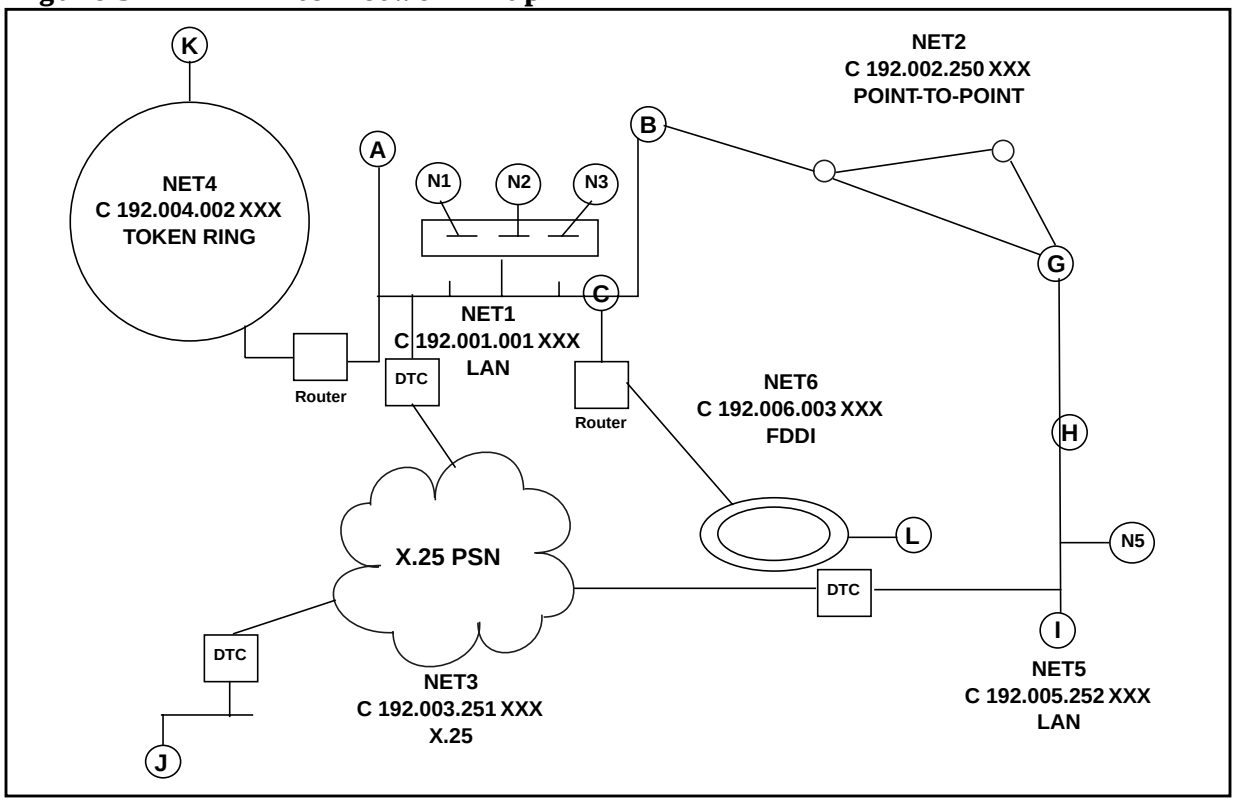
An **internetwork map** provides information about the whole internetwork. Figure 3-1 is an example of an internetwork map. This sample internetwork will be used throughout the instructions in this chapter to help explain the other drawings and tables that make up the configuration worksheets.

Before you can draw your internetwork map, you must know how many networks your internetwork will contain, and you must know each network type (ThinLAN, Token Ring, FDDI, 100VG-AnyLAN, 100Base-T, NS Point-to-Point, or X.25). The internetwork in the example (Figure 3-1) contains six networks. NET1 and NET5 are LANs, NET1 is 100Base-T LAN and NET5 is a ThinLAN, NET2 is a Point-to-Point network, NET3 is an X.25 network, NET4 is a Token Ring network, and NET6 is an FDDI network.

NOTE

If you have an X.25 network, you should indicate the presence of each Datacomm and Terminal Controller (DTC) in your internetwork map, as shown in this example (Figure 3-1). Both the NS 3000/iX node and the DTC must be specially configured for X.25 links.

Figure 3-1 Internetwork Map



Communication Between Networks

Since the main purpose of the internetwork map is to show how networks are connected, gateway nodes are the only nodes you should label on the internetwork map. All other nodes and their networks can be represented by drawing sketches of the networks, as shown in Figure 3-1. In the example, node B is a full gateway that belongs to NET1 and NET2, node A is a full gateway that belongs to NET1 and NET4, and node C is a full gateway that belongs to NET1 and NET6. Nodes G and H are gateway halves that belong to NET2 and NET5, respectively.

NOTE Single letters are used to represent node names in this example. Actual node names must be in an accepted format. They may be either in the form `nodename.domain.organization` or they may be in a valid domain name format.

Network Boundaries

Once you have drawn your gateway nodes and routers, you have established network boundaries. Consider the example and look at Figure 3-1. Since node B in the example is a full gateway and belongs to both NET1 and NET2, the boundary between these two networks is at node B itself. The boundary between NET2 and NET5 is along the gateway-half link that connects gateway nodes G and H.

IP Network Addresses

Each network in your internetwork must have a unique IP network address. Add these IP addresses to your internetwork map.

In the example, assume that the Class C IP network addresses are those shown in Figure 3-1. The specific IP node addresses do not need to be shown until completion of specific parts of the network worksheets, so node portions of IP addresses will be represented with XXX in some maps and tables.

Completing the Internetwork Table

Once your internetwork map contains the information just described, you are ready to complete the internetwork table (Table 3-1).

The information requested for the first three columns of the internetwork table can be taken directly from the internetwork map, as in the example. In the Implementation Priority column, consider which networks must be operational immediately. You also may want to consider which networks will be the easiest to initiate. Analyzing these and other factors important to you, determine the order in which you plan to initiate your networks, and then enter the information in the Implementation Priority column of the internetwork table.

When you have completed both the internetwork map and the internetwork table, you have finished the internetwork worksheets.

Table 3-1 Internetwork Table

NETWORK	NETWORK TYPE (LAN, PT–PT, X.25, TOKEN RING)	IP NETWORK ADDRESS	IMPLEMENTATION PRIORITY
NET1	LAN	C 192.001.001 XXX	1
NET2	NS POINT-TO-POINT	C 192.002.250 XXX	2
NET3	X.25	C 192.003.001 XXX	3
NET4	TOKEN RING	C 192.004.001 XXX	4
NET5	LAN	C 192.005.001 XXX	5
NET6	FDDI	C 192.006.001 XXX	6

Drawing a Network Map

A **network map** provides information about the configuration of the computers on the network and their access to remote computers. A network map can be invaluable when troubleshooting.

Whenever you install a new system on your network, be sure you also update your network map. If you have not previously created a network map, create one now and keep it updated whenever you add or delete computers or interface cards or make cable changes.

In addition to maintaining a network map, you should also record related system information on one of the network map worksheets, provided later in this chapter. You can use the network map worksheet as a guide for configuration and later as a record of your configuration for both you and your HP support staff.

Network Worksheets

For each network in your internetwork, you are asked to draw a map of the network and to complete two tables. One table lists node-specific information, and one table lists network routing information.

You also are asked to complete worksheets for each gateway half pair in your internetwork. The worksheets for a gateway half pair consist of a map of the gateway half nodes and their connecting link and a table containing information about the gateway half network interfaces.

In the sample internetwork shown in Figure 3-1, six sets of network worksheets need to be completed: one set for each of the six networks and one set for the gateway half pair.

Take the following steps when filling out a set of network worksheets:

1. Draw your map, showing all nodes and node names. For Point-to-Point networks, also show all Point-to-Point links and link names.
2. Complete the two tables: for each network, for a gateway-half pair, include the link name.

LAN Network Worksheets

One set of LAN network worksheets should be used for each LAN in your internetwork. The LAN network worksheets consist of a map of the LAN and two tables. One table contains information about each node on the LAN and one table contains network-specific internet routing information.

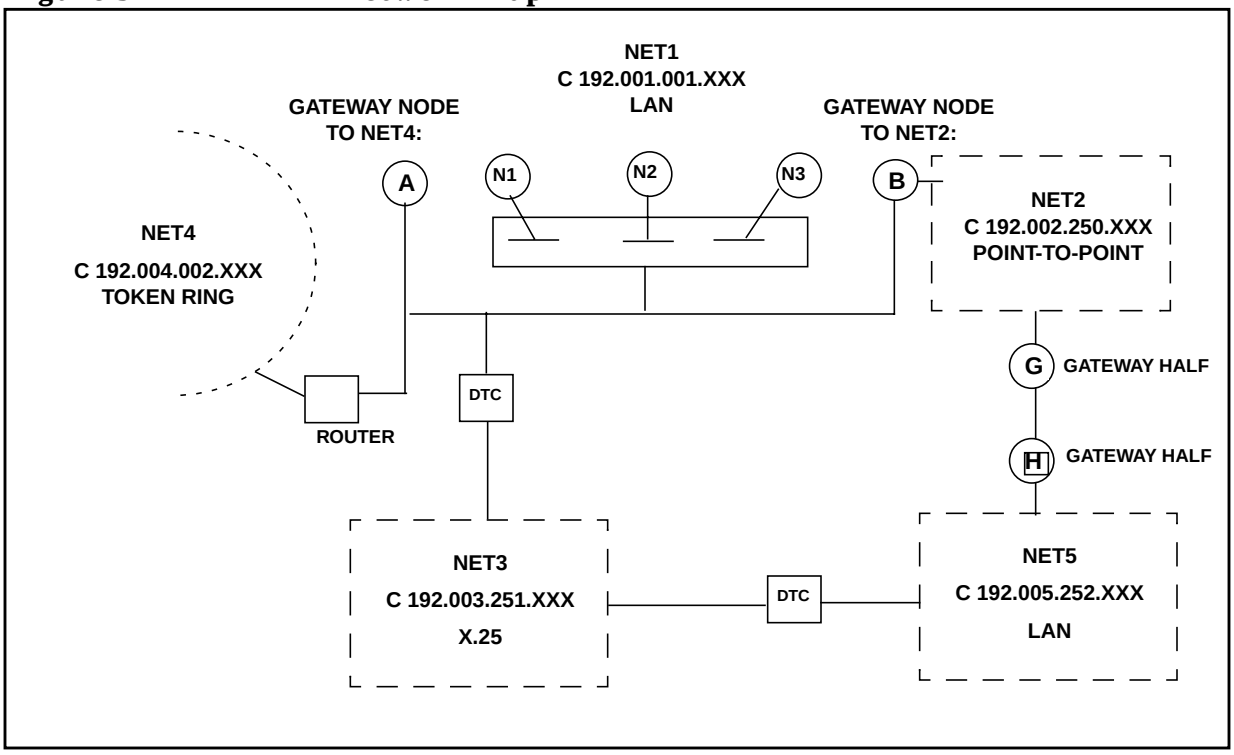
In this example, we have shown the network map and worksheet for NET1, one of the LAN networks shown in Figure 3-1. Use the discussion of the sample LAN network worksheets as a guide for filling out your own LAN network worksheets.

LAN Network Map

Figure 3-2 is a drawing of the network map for NET1. The network map is a detailed drawing of the same network shown in the internetwork map (Figure 3-1). The network name, the IP network address, and the network type are listed at the top of the network map.

In the example, the internetwork map shows that node B is a gateway node. It is noted on the NET1 network map and shows the network that the gateway node can reach. Node B is also a proxy server. The remaining NET1 nodes and their names are added to the network map.

Figure 3-2 LAN Network Map



LAN Network Table

Refer to the LAN network map to fill in the LAN network table (Table 3-2). The first column lists the names of all the nodes on NET1. Each node is assigned an IP address that is unique within the network. Only the node portion of the IP address is listed since the IP network address is noted at the top of the table. In the third column of Table 3-2, node B is shown as a proxy server. The fourth column lists node B as a gateway node. In the Implementation Priority column, the nodes are ranked in the recommended order of configuration.

Table 3-2 LAN Network Table

NETWORK NAME:	**NET1**			
IP NETWORK ADDRESS	**C 192.001.001 XXX**			
NODE NAME	**IP NODE ADDRESS**	**PROXY SERVER (Y/N)**	**GATEWAY NODE (Y/N)**	**IMPLEMENTATION PRIORITY**
A	001			2
L1	002			3
L2	003			4
L3	004			5
B	005	YES	YES	1

LAN Internet Routing Table

The purpose of the LAN internet routing table (Table 3-3) is to list all possible networks that can be reached from each gateway node on a LAN, such as NET1 in the example.

As shown on the internetwork map, NET1 includes a neighbor gateway node B. In the IP Node Address column of the LAN internet routing table, the node portion of the gateway node's IP address is listed. The LAN internet routing table shows that NET1 nodes using node B as a gateway can reach NET2 in one hop, NET5 in two hops, and NET3 in three hops. Node B is also designated as a default gateway.

Table 3-3 LAN Internet Routing Table

NETWORK NAME:		**NET1**		
IP NETWORK ADDRESS		**C 192.001.001 XXX**		
GATEWAY	**IP NODE ADDRESS**	**DESTINATION**	**HOPS TO DESTINATION**	**DEFAULT GATEWAY (Y/N)**
B	005	NET2 C 192.002.250 XXX	1	YES
		NET5 C 192.005.252 XXX	2	
		NET3 C 192.003.251 XXX	3	

Token Ring Network Worksheets

You may use the worksheets found in the LAN section for Token Ring. It is important to note that Token Ring does not use a proxy server.

FDDI Network Worksheets

You may use the worksheets found in the LAN section for FDDI as well. It is important to note that FDDI does not use a proxy server.

100VG-AnyLAN Network Worksheets

You may use the worksheets found in the LAN section for 100VG-AnyLAN.

100Base-T Network Worksheets

You may use the worksheets found in the LAN section for 100Base-T.

Point-to-Point Network Worksheets

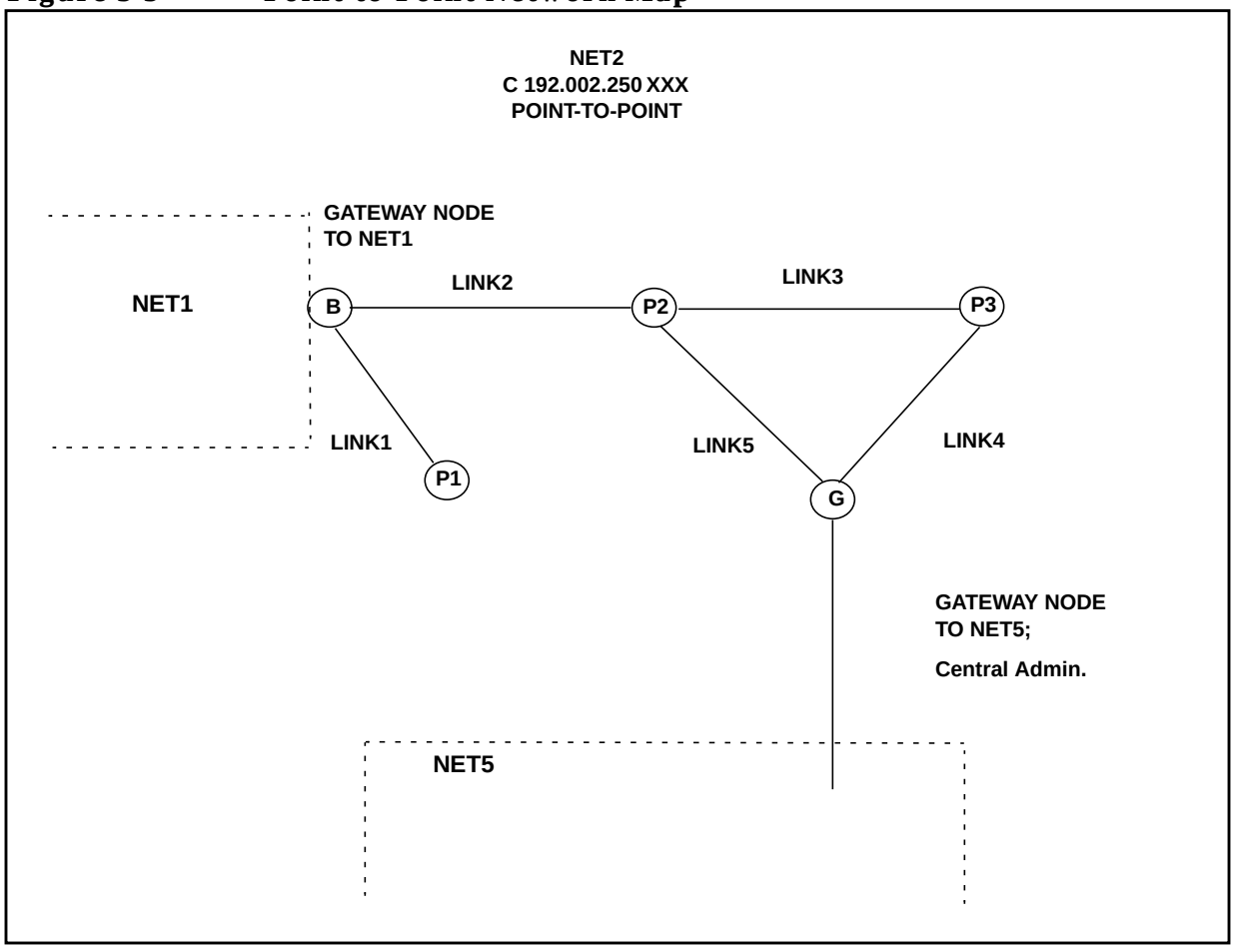
One set of Point-to-Point network worksheets should be used for each Point-to-Point network in your internetwork. These network worksheets consist of a map of the Point-to-Point network and two tables. One table contains information about each node on the network and one table contains network-specific internet routing information.

Point-to-Point Network Map

NET2 is the Point-to-Point network in the sample internetwork. Figure 3-3 is a drawing of the network map for NET2. The network map is a detailed drawing of the same network shown in the internetwork map (Figure 3-1). The network name, the IP network address, and the network type are listed at the top of the network map. This information is derived from the internetwork map.

The internetwork map shows that nodes B and G are gateway nodes and also shows the networks that the gateway nodes can reach. The remaining NET2 nodes and their names are added to the network map. Node G is a central administrative node.

Figure 3-3 Point-to-Point Network Map



Point-to-Point Network Table

Refer to the Point-to-Point network map to fill in the Point-to-Point network table (Table 3-4). We have completed the first column by listing the names of all the nodes on NET2. Each node is assigned an IP address that is unique within the network. Only the node portions of the IP addresses are listed because we have listed the IP network address at the top of the table. In the third column of Table 3-4, note that node G is a central administrative node. In the fourth column, nodes B and G are indicated as gateway nodes. For the Implementation Priority column, the nodes are ranked in the recommended order of configuration.

Table 3-4 Point-to-Point Network Table

NETWORK NAME:	**NET2**			
IP NETWORK ADDRESS	**C 192.002.250 XXX**			
NODE NAME	**IP NODE ADDRESS**	**PROXY SERVER (Y/N)**	**GATEWAY NODE (Y/N)**	**IMPLEMENTATION PRIORITY**
B	001		YES	2
P1	002			3
P2	003			4
P3	004			5
G	005	YES	YES	1

Point-to-Point Internet Routing Table

The purpose of the Point-to-Point internet routing table (Table 3-5) is to list all possible networks that can be reached from each gateway node on a Point-to-Point network, which is NET2 in the example. (Note that there may be more than one route to a network.)

As shown on the internetwork map, NET2 includes two gateway nodes, B and G. In the IP Node Address column of the Point-to-Point internet routing table, the node portion of each gateway node's IP address is listed. The Point-to-Point internet routing table indicates that NET2 nodes using node B as a gateway can reach NET1 in one hop, NET4 in two hops, and so on.

For Node G, the same type of information is listed.

Table 3-5 Point-to-Point Internet Routing Table

NETWORK NAME:		NET2	
IP NETWORK ADDRESS		C 192.002.250 XXX	
GATEWAY	**IP NODE ADDRESS**	**DESTINATION**	**HOPS TO DESTINATION**
B	001	NET1 C 192.001.001 XXX	1
		NET4 C 192.004.002 XXX	2
		NET3 C 192.003.251 XXX	2
		NET5 C 192.005.252 XXX	3
		NET6 C 192.006.003 XXX	2
G	005	NET5 C 192.005.252 XXX	1
		NET3 C 192.003.251 XXX	2
		NET1 C 192.001.001 XXX	3
		NET4 C 192.004.002 XXX	4
		NET3 C 192.003.003 XXX	4

X.25 Network Worksheets

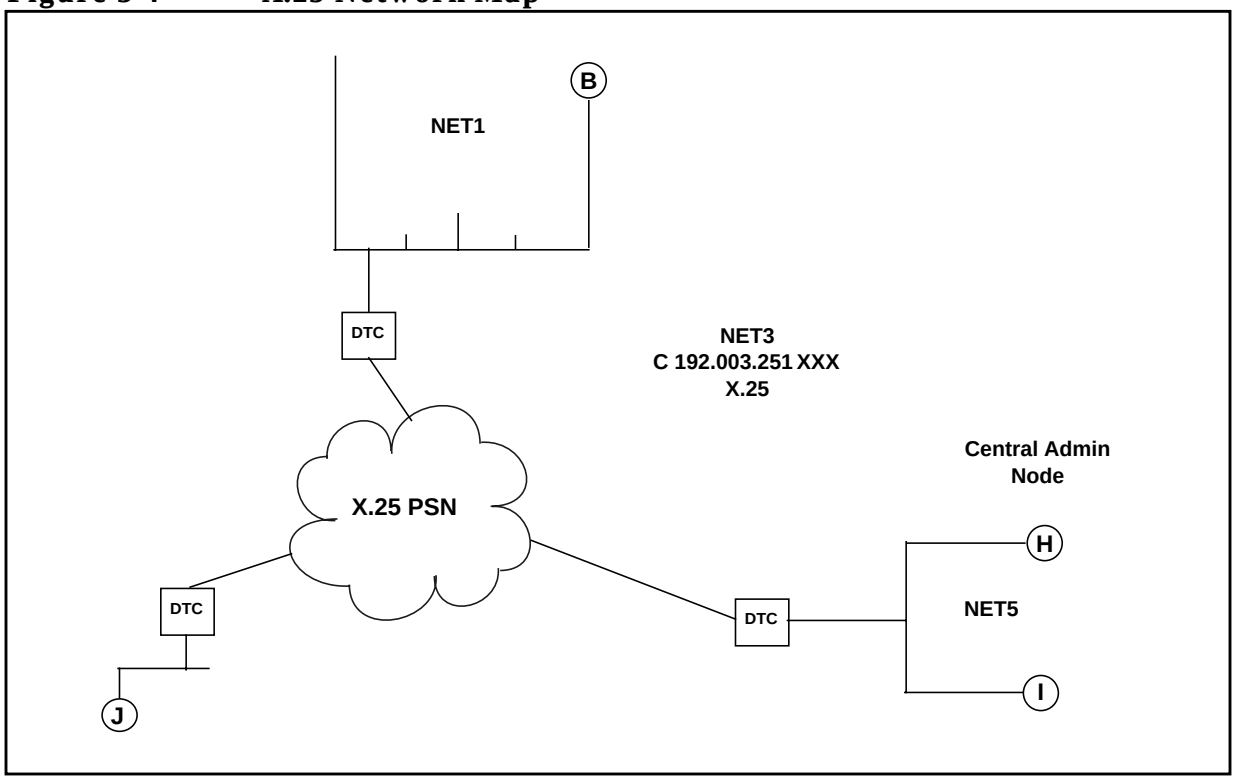
One set of X.25 network worksheets should be used for each X.25 network in your internetwork. The X.25 worksheets consist of a map of the X.25 network and two tables. One table contains information about each node on the X.25 network. The other table contains network-specific internet routing information.

X.25 Network Map

Figure 3-4 is a drawing of the network map for NET3. The network map is a detailed drawing of the same network shown in the internetwork map (Figure 3-1). The network name, the IP address, and the network type are shown on the network map. This information is derived from the internetwork map.

In the example, node B of NET1 and nodes H and I of NET5 are also part of the X.25 network. The remaining NET3 nodes and their names are added to the network map. The network map also shows node H as a central administrative node.

Figure 3-4 X.25 Network Map



X.25 Network Table

Refer to the X.25 network map to fill in the X.25 network table as shown in Table 3-6. We complete the first column by listing the names of all the nodes on NET3. Each node is assigned an IP address that is unique within the network. Only the node portions of the IP addresses are listed since the IP network address is listed at the top of the table. In the third column of the table, node H is indicated as a central administrative node. The X.25 (subnet) address for each node is listed in the fifth column of the network table. The X.25 address is a decimal number (up to 15 digits) identifying a node's location on the X.25 subnet for connections using switched virtual circuits (SVCs). Usually this address is inserted in CALL packets to set up connections using SVCs. If the network you will access is a public packet switching network (PSN), these addresses (where appropriate) are recorded on the network subscription form.

Table 3-6 X.25 Network Table

NETWORK NAME:		NET3	
IP NETWORK ADDRESS		C 192.003.251 XXX	
NODE NAME	**IP NODE ADDRESS**	**CENTRAL ADMIN NODE (Y/N)**	**X.25 ADDRESS**
H	001	Y	1234
I	002		5678
J	003		6879
B	004		9876

X.25 Internet Routing Table

The purpose of the X.25 internet routing table (Table 3-7) is to list the other networks in the internetwork that can be reached from the X.25 network, which is NET3 in the example. (Note that there may be more than one route to a network.)

As shown in the internetwork map (Figure 3-4), NET3 includes two gateway nodes, B and H. In the X.25 internet routing table note that NET3 nodes using Node H can reach NET5 in one hop, NET2 in two hops, and so on. In the IP Node Address column, the node portion of the node's IP address is listed.

Table 3-7 X.25 Internet Routing Table

NETWORK NAME:		NET3	
IP NETWORK ADDRESS		C 192.003.251 XXX	
GATEWAY	**IP NODE ADDRESS**	**DESTINATION**	**HOPS TO DESTINATION**
B	004	NET1 C 192.001.001 XXX	1
		NET4 C 192.004.002 XXX	2
		NET2 C 192.002.250 XXX	2
		NET5 C 192.005.252 XXX	3
H	001	NET5 C 192.005.252 XXX	1
		NET2 C 192.002.250 XXX	2
		NET1 C 192.001.001 XXX	3
		NET4 C 192.004.002 XXX	4

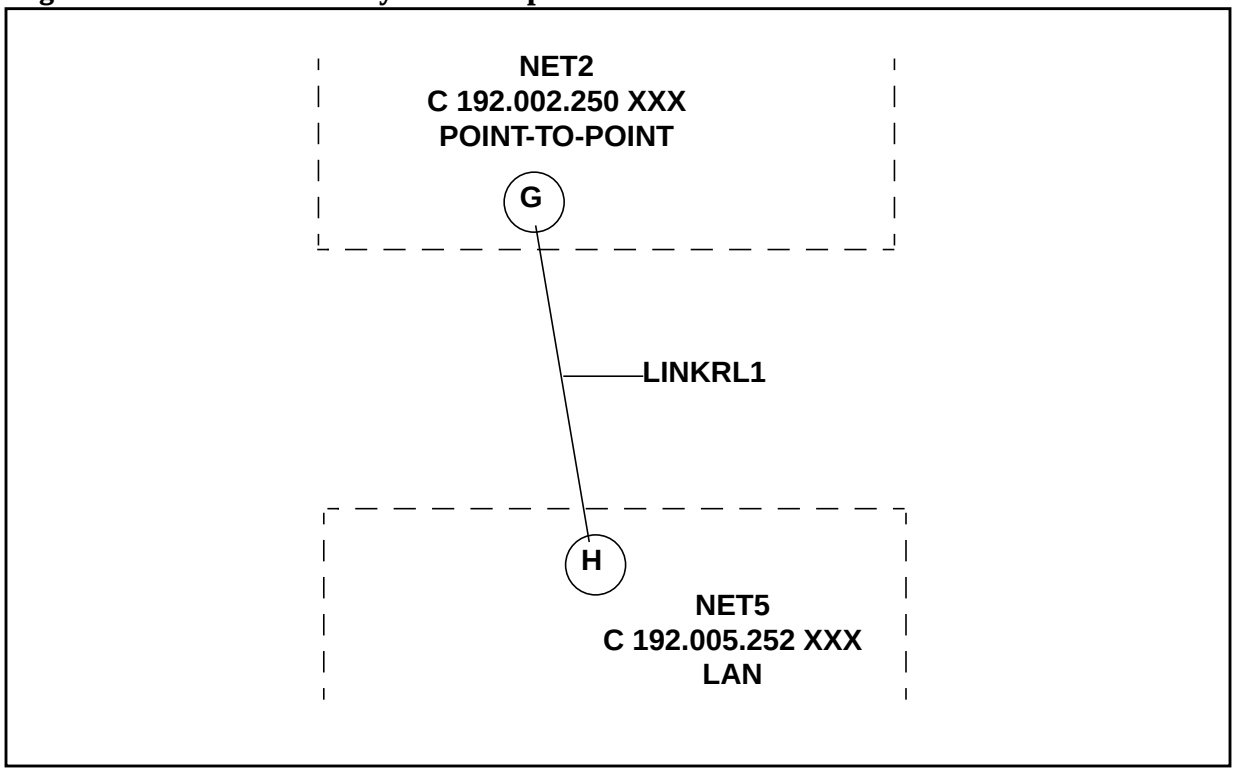
Gateway Half Pair Worksheets

One set of gateway half pair worksheets should be used for each gateway half pair in your internetwork. The gateway half pair worksheets consist of a map of the two gateway half nodes and their connecting link, and one table that contains information about the gateway half network interfaces. In the sample internetwork shown in Figure 3-1, nodes G and H form a gateway half pair. Use the discussion of the sample gateway half pair worksheets as a guide for filling out your own gateway half pair worksheets.

Gateway Half Map

The sample internetwork contains one gateway half pair, as shown in the internetwork map, which is made up of nodes G and H and their connecting link. Figure 3-5 is a drawing of the gateway half pair showing the two nodes and the networks to which they belong. In addition, the map shows the link name, LINKRL1.

Figure 3-5 Gateway-Half Map



Gateway Half Network Interface Table

Table 3-8 is based on the map discussed in the previous section. Both gateway half nodes, the full IP addresses of the partner nodes, the connected networks, and the name of the link are listed. Usually, the link name will be the same from the perspective of each gateway half. The address of the partner gateway half is shown to demonstrate that the partner's address is entered during configuration of a gateway half network interface.

Table 3-8 Gateway Half Network Interface Table

NETWORK NAMES:		NET2, NET3	
GATEWAY HALF NODE	**FULL IP ADDRESS OF PARTNER**	**CONNECTED NETWORK**	**LINK NAME**
G/NET2	C 192.005.250 005	NET5	LINKRL1
H/NET5	C 192.002.252 001	NET2	LINKRL1

Network Directory Worksheet

You can complete the network directory information table shown below for each network directory you are configuring. For your node and for each destination node, you must make a full entry in the network directory. The entry includes the destination node's name and IP address, its NI type, the global/local setting, and any additional address that is required based on the NI type. See Chapter 11 , “Configuring the Network Directory,” for more information on NI types and additional addresses. Table 3-9 shows some of the network directory entries you might configure for node B of the internetwork shown in Figure 3-1.

Table 3-9 Network Directory Information Table

NODE NAME	GLOBAL OR LOCAL	IP ADDRESS	TYPE	ADDITIONAL ADDRESS
H	GLOBAL	C 192.005.252 001	1	
I	LOCAL	C 192.005.252 002	1	
J	GLOBAL	C 192.005.251 003	3	6879
A	GLOBAL	C 192.001.001 001	5	08-00-09-11-22-11
K	GLOBAL	C 192.004.002 001	1	

4 Planning for Node Configuration

This chapter describes how to complete node worksheets before you start configuration. You will need to collect some information ahead of time to complete these tasks.

The main purpose of the node worksheets is to determine the information you will need to configure for each node during NMMGR's guided configuration. This information depends on the type of network you have. For a description of the fields in these worksheets, see Chapter 6 , "Configuring a LAN Node," for information on LAN, Token Ring, and FDDI, and Chapter 7 , "Configuring a Point-to-Point Node," for information on Point-to-Point and Chapter 8 , "Configuring a X.25 Node," for information on X.25.

It is recommended that you make copies of these worksheets and fill in the parameter information, then use these worksheets to guide you through configuration in NMMGR.

Node worksheets list only the fields you can configure during guided configuration, which allows you to configure your nodes as quickly as possible. For information on configuration parameters that are available through non-guided configuration, see the *NS 3000/iX NMMGR Screens Reference Manual*.

This chapter includes:

- Node worksheet information.
  - — Node worksheet information.
  - — Token Ring configuration worksheet
  - — FDDI configuration worksheet.
  - — 100VG-AnyLAN configuration worksheet.
  - — 100Base-T configuration worksheet.
  - — Point-to-Point configuration worksheet.
  - — X.25 configuration worksheet.
  - — X.25 virtual circuit configuration worksheet.
- Neighbor gateway worksheet information.
  - — Neighbor gateway configuration worksheet.
- Neighbor gateway reachable networks worksheet Information.
  - — Neighbor gateway reachable networks configuration worksheet.

Node Worksheet Information

Table 4-1, has a description of the information that needs to be gathered for the worksheets that are in this chapter. Check the worksheets to see which is the appropriate information to gather. This information is used in the configuration chapters of this manual.

Table 4-1 Configuration Worksheet Information

Field	Screen	Description
Address key	X.25 Virtual Circuit Configuration	In the network directory, the name of each node listed in the remote node name field. HP recommends that you use the node portion of the remote node's node name as the address key.
Card number	X.25 Configuration	Slot number of the DTC/X.25 Network Access card.
DTC node name	X.25 Configuration	Node name of the DTC in the form `node.domain.organization`. Must agree with node name configured through during configuration of the datacommunications and terminal subsystem (DTS). The node name must be entered for each DTC/X.25 network access card that allows system-to-system connections.
Enable ethernet/ Enable IEEE 802.3	LAN Configuration	Both ethernet and IEEE 802.3 are enabled by default. You may disable one or the other but not both (one must be enabled). To disable either ethernet or IEEE 802.3, enter an `N` (no) in the field next to the enable question.
Facility set	X.25 Virtual Circuit Configuration	For SVCs only. A name for a collection of X.25 connection parameters in the network directory. Use the default (STDSFSET) or enter a different name, then go to Facility sets to define parameters. It must match the parameters specified by your network subscription.

Table 4-1 Configuration Worksheet Information

Field	Screen	Description
IP address	LAN Configuration; Token Ring Configuration; FDDI Configuration; Point-to-Point Configuration; X.25 Configuration	There are two methods of entering an internet protocol (IP) address within NMMGR: 1. Enter the fully qualified IP address (for example, Class C, `C 192.191.191 009`). OR 2. Enter only the network (*nnn*) and node (xxx) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, `15.123.44.98`). You need not enter the following items as NMMGR will fill these in: a. Class A, B, C b. Leading zeros for the network and node portion of the IP address. All nodes on the same network must use the same class of IP address. The network portion of the address must be the same for all nodes on the same network.
IP subnet mask	LAN Configuration; Token Ring Configuration; FDDI Configuration; Point-to-Point Configuration; X.25 Configuration	The IP subnet mask is optional. An IP subnet mask is specified in the same format as an IP address. The mask identifies which bits of an IP address will be used to define a subnetwork. For more information refer, to the configuration chapter for the type of link you are configuring.
Link name		The link name represents a hardware interface card. This name must be unique to both the node and the network. The link name can have up to eight alphanumeric characters and the first character must be alphabetic.
(LAN Link name)	LAN Configuration	This represents the LAN card for which you are configuring a link.
(Token Ring Link name)	Token Ring configuration	This represents the Token Ring card for which you are configuring a link.

Table 4-1 Configuration Worksheet Information

Field	Screen	Description
(FDDI Link name)	FDDI Configuration	This represents the FDDI card for which you are configuring a link.
(100VG-AnyLAN Link name)	LAN Configuration	This represents the 100VG-AnyLAN card for which you are configuring a link.
(100Base-T Link name)	LAN Configuration	This represents the 100Base-T card for which you are configuring a link.
(X.25 Link name)	X.25 Configuration	The name of the link used by X.25 iX System Access. It must match the link name configured during configuration of the datacommunications and terminal subsystem (DTS).
(Point-to-Point Link name)	Point-to-Point Configuration	This represents the PSI card for which you are configuring a link.
Local node name	Main	The node name is the name by which the HP e3000 computer is known in the network. The format of a node name is `nodename.domain.organization` where the total number of characters is 50 or fewer, and each field contains 16 or fewer characters (alphanumeric, underscore, or hyphens). The first character of each field must be alphabetic.
Local domain name	NS Configuration	The name of the system in ARPANET standard format. It is composed of labels, with each label separated by a period. Labels must start with a letter or digit and have as interior characters only letters, digits, hyphens(-), or underbars (_). There may be any number of labels, but the total length of the name, including periods, is limited to 255 characters. (If not using domain names for network access, leave the local node name in this field.)

Table 4-1 Configuration Worksheet Information

Field	Screen	Description
Network directory name	X.25 Virtual Circuit Configuration	The network directory name must be configured for each new node. The network directory contains information that one node needs in order to communicate with other nodes. The only network directory name supported by HP is `NSDIR.NET.SYS`.
Network Interface (NI) name	LAN Configuration; Token Ring Configuration; FDDI Configuration; Point-to-Point Configuration; X.25 Configuration	The network interface (NI) name is used to easily identify a network interface. The name can be up to eight alphanumeric characters, starting with a letter. The maximum number of NIs that can be configured on a node is 48. If a node interfaces to more than one network, give each NI on that node a unique name. You will use the NI name with the `NETCONTROL` command to start the transport and network link.
Permanent VC number	X.25 Virtual circuit Configuration	For PVCs only. In the network directory, the number of the permanent virtual circuit on the remote node.
Physical path	Point-to-Point Configuration	This is the location of the programmable serial interface. Refer to Chapter 7 , “Configuring a Point-to-Point Node,” for further details regarding physical path.
Physical path of LANIC	LAN Configuration	This is the location of the LANIC device adapter card. Refer to the LAN section of Chapter 6 , “Configuring a LAN Node,” for further details regarding physical path.
Physical path of device adapter	FDDI Configuration	This is the location of the FDDI device adapter card. Refer to the FDDI section of Chapter 6 , “Configuring a LAN Node,” for further details regarding the physical path.
Physical path of Token Ring device adapter	Token Ring Configuration	This is the location of the Token Ring device adapter card. Refer to the Token Ring section of Chapter 6 , “Configuring a LAN Node,” for further details regarding physical path.

Table 4-1 Configuration Worksheet Information

Field	Screen	Description
Proxy node	LAN Configuration	The proxy field is optional. Enter Y (yes) only if your network has internetworks (networks with gateways) or non-HP nodes. Establishing a proxy node is a way of placing node name and address mapping information in a single location. For more information, see the configuration chapter for LAN link.
Remote IP address	X.25 Virtual Circuit Configuration	In the network directory, the IP address of each node listed in the remote node name field.
Remote node name	X.25 Virtual Circuit Configuration	In the network directory, the name of each remote X.25 node on the network
Remote X.25 address	X.25 Virtual Circuit Configuration	For SVCs only. In the network directory, the X.25 address of the remote host for X.25 public data networks or private networks.
Security class	X.25 Virtual Circuit Configuration	For SVCs only. In the network directory, the security to be applied for connection establishment with the remote node.
Speed	Point-to-Point Configuration	The line transmission speed is given in bits per second. For direct connect the value must be supported by the cable. Values are 1200, 2400, 4800, 9600, 19200, 38400, 56000, and 64000. The default is 56000.
Type	Point-to-Point Configuration	Enter DD (direct dial) if you always want to call the same host over a dial link. If you choose DD the remote host does not have to be adjacent and other nodes can be accessed through the remote host. Enter SD if you want to call more than one adjacent remote node over a dial link without reconfiguring. If you choose SD, no other remote nodes can be accessed through the remote host; it is an end point in the connection. Enter DC if the link is a leased line, private line, or other non-switched link.

LAN Configuration Worksheet

Fill out the following worksheet (Figure 4-1) for each LAN link you are configuring.

Figure 4-1 LAN Configuration Worksheet

LAN Configuration Worksheet

Node Name _____

Network Interface (NI) name _____

IP address _____

IP subnet mask_____ (optional)

Proxy name_____ (Y/N)

Node Name _____

Link type _____ (BT100, VG100LAN, LAN)

Physical path of LANIC _____

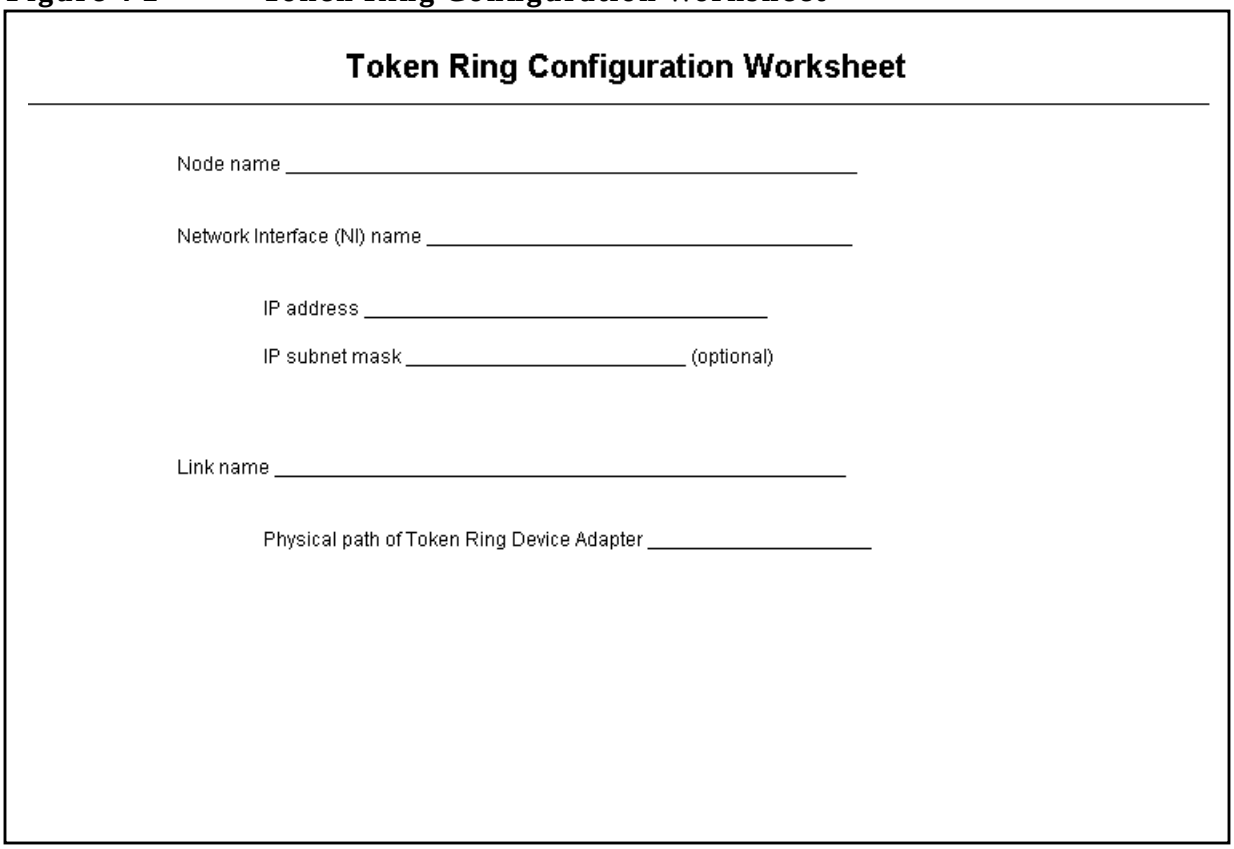
Enable Ethernet _____ (Y/N)

Enable IEEE 802.3 _____ (Y/N)

Token Ring Configuration Worksheet

Fill out the following worksheet (Figure 4-2) for each Token Ring link you are configuring.

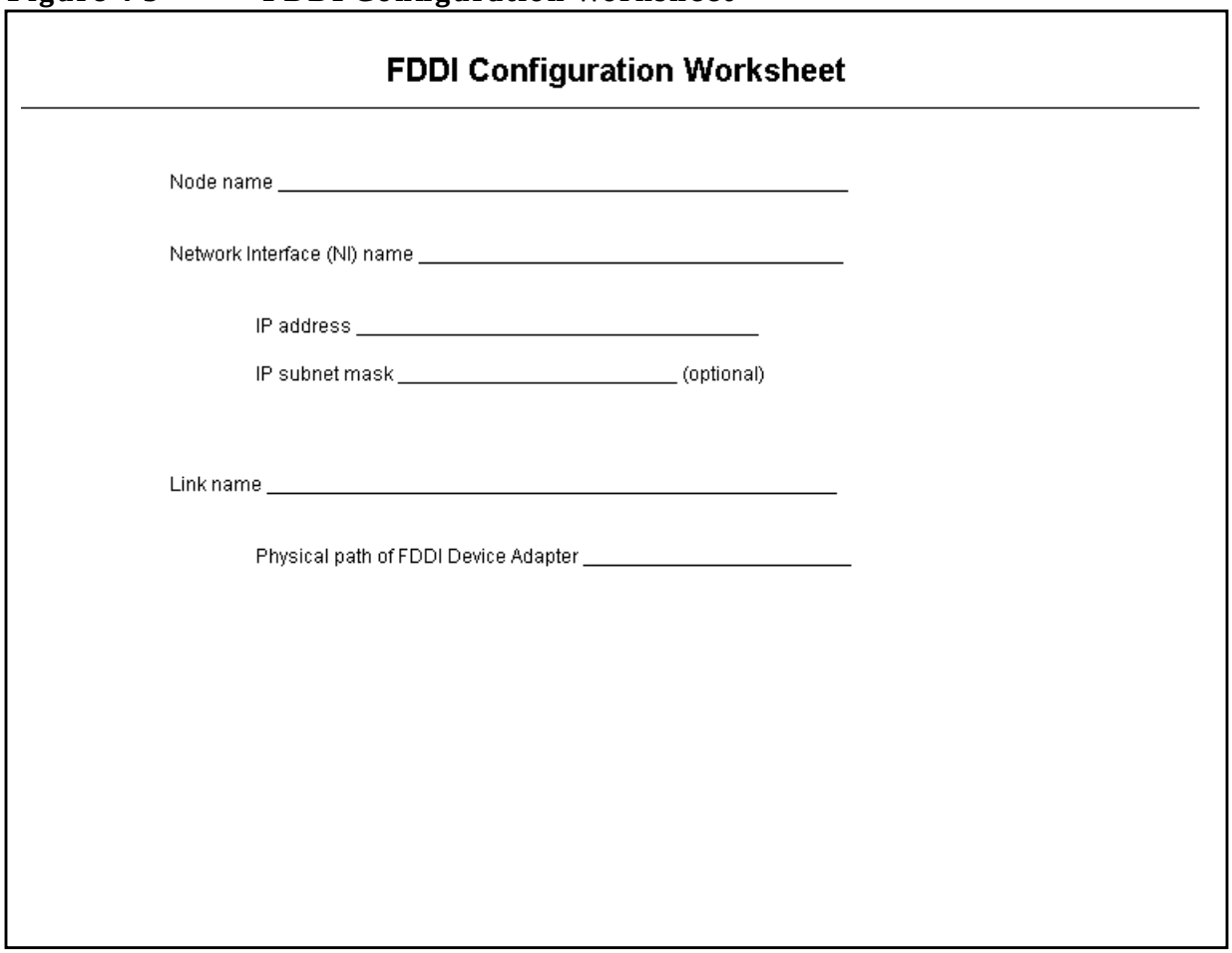
Figure 4-2 Token Ring Configuration Worksheet



FDDI Configuration Worksheet

Fill out the following worksheet (Figure 4-3) for each FDDI link you are configuring.

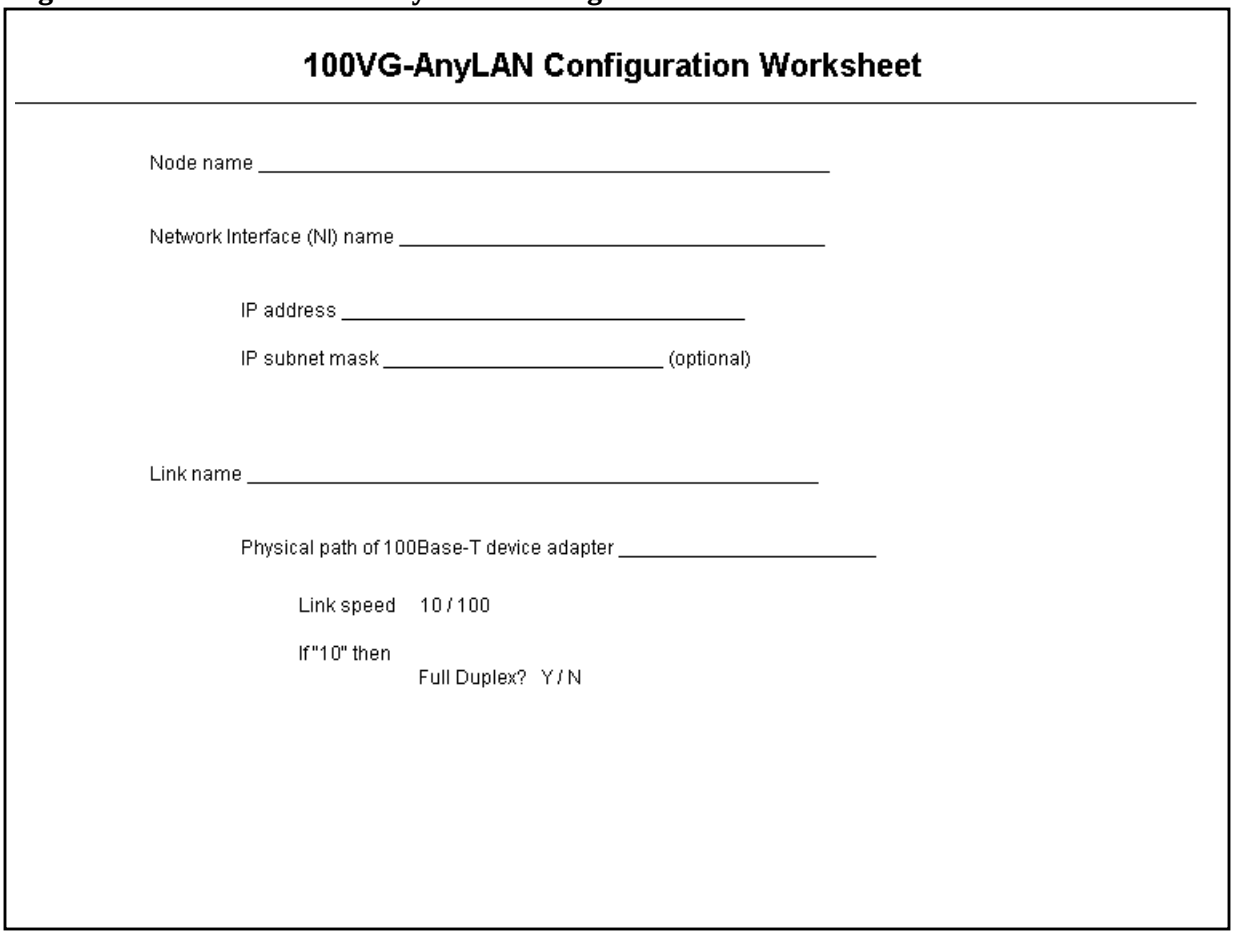
Figure 4-3 FDDI Configuration Worksheet



100VG-AnyLAN Configuration Worksheet

Fill out the following worksheet (Figure 4-4) for each 100VG-AnyLAN link you are configuring.

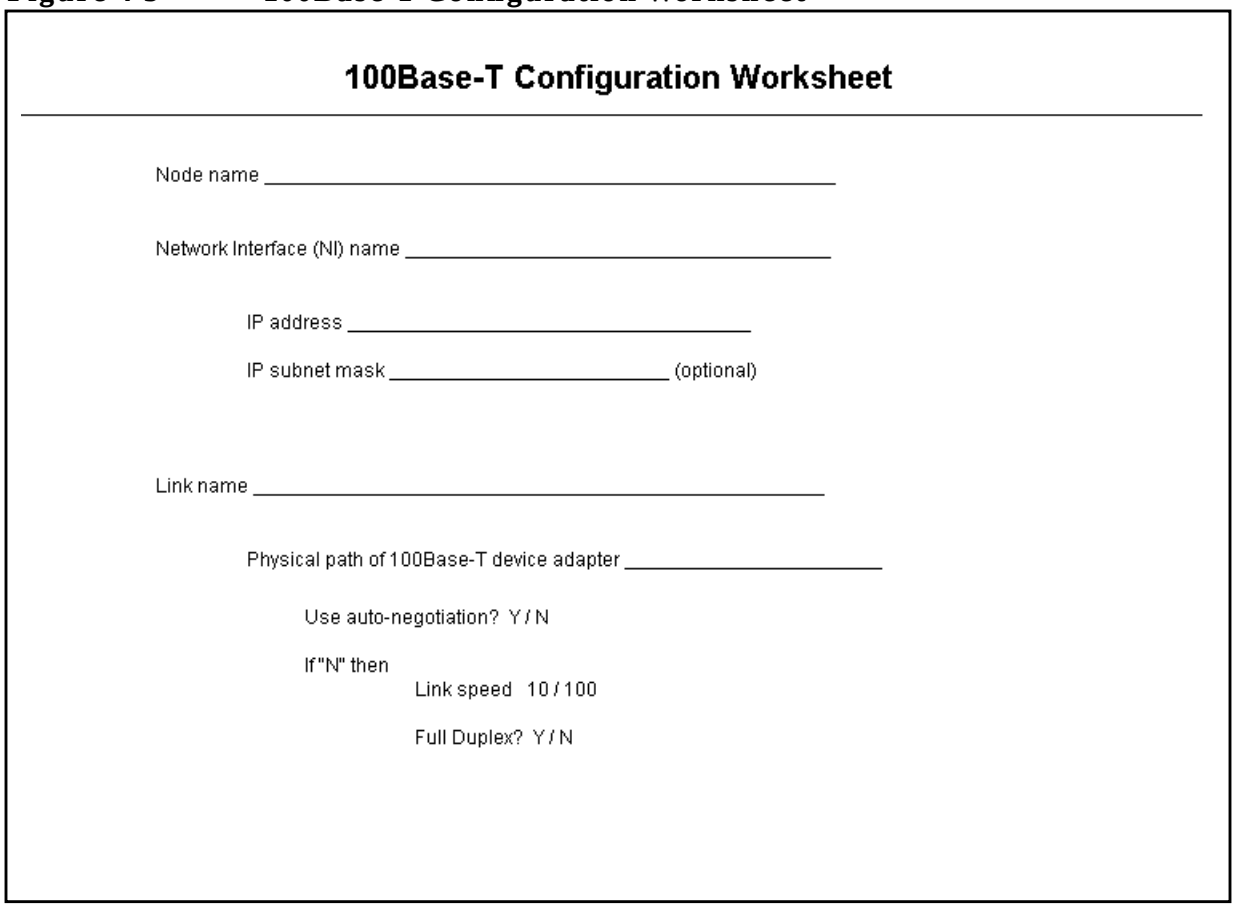
Figure 4-4 100VG-AnyLAN Configuration Worksheet



100Base-T Configuration Worksheet

Fill out the following worksheet (Figure 4-5) for each 100Base-T link you are configuring.

Figure 4-5 100Base-T Configuration Worksheet



Point-to-Point Configuration Worksheet

Fill out the following worksheet (Figure 4-6) for each Point-to-Point link you are configuring.

Figure 4-6 Point-to-Point Configuration Worksheet

Point-to-Point Configuration Worksheet

Node Name _____ (Specify local system)

Network Interface (NI) name _____

IP address _____IP subnet mask _____ (optional)

Link name	Link type (LAPBMUX or LAPB)	Physical Path	Speed	Type

X.25 Configuration Worksheet

Fill out the following worksheet (Figure 4-7) for each X.25 link you are configuring.

Figure 4-7 X.25 Configuration Worksheet

X.25 Configuration Worksheet

Node name _____ (Specify local system)

Network Interface (NI) name _____

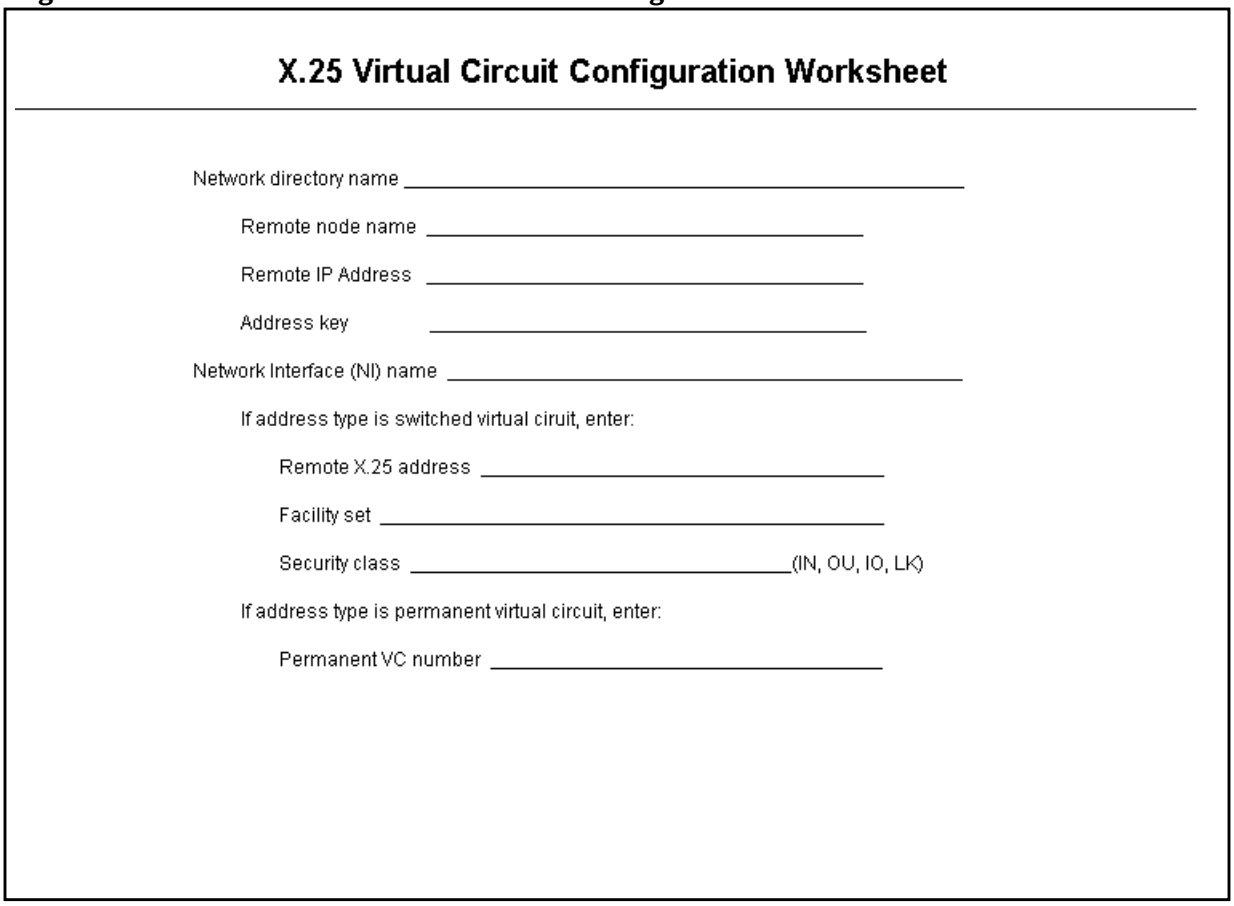
IP address _____ IP subnet mask _____(optional)

Link name	DTC Node Name	Card Number

X.25 Virtual Circuit Configuration Worksheet

Fill out the following worksheet (Figure 4-8) for each X.25 Virtual Circuit you are configuring.

Figure 4-8 X.25 Virtual Circuit Configuration Worksheet



Neighbor Gateway Worksheet Information

The following is a description of the information that needs to be gathered for the worksheets that follow in this chapter. This information is used for configuring nodes.

`Gateway name`

Enter the name of a gateway that is on the same network as the node that you are configuring. (Nodes are on the same network if the network portions of their IP addresses are the same.) Each gateway name can be as long as eight alphanumeric characters. The first character must be alphabetic

`New name`

Enter the name of a gateway that is on the same network as the node that you are configuring. (Nodes are on the same network if the network portions of their IP addresses are the same.) Each gateway name can be as long as eight alphanumeric characters. The first character must be alphabetic.

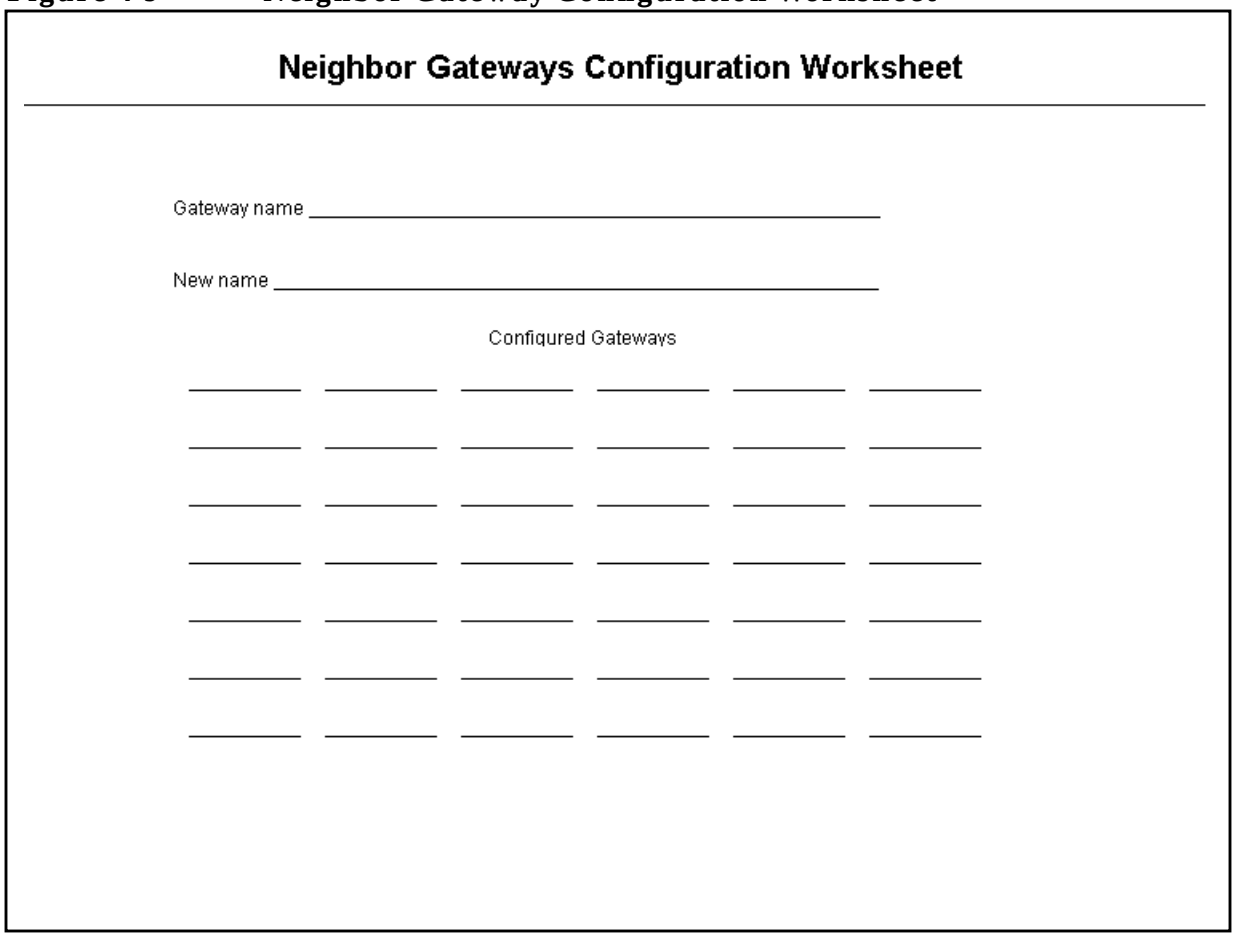
`Configured Gateways`

This is a list of gateways that are configured. Gateway names are automatically entered in these fields when they are entered above.

Neighbor Gateway Configuration Worksheet

Fill out the following worksheet (Figure 4-9) for each neighbor gateway you are configuring.

Figure 4-9 Neighbor Gateway Configuration Worksheet



Neighbor Gateway Reachable Networks Worksheet Information

The following is a description of the information that needs to be gathered for the worksheets that follow in this chapter. This information is used for configuring nodes.

`Neighbor Gateway IP Internet Address`

This is the IP address of the gateway specified on the Neighbor Gateways screen. The IP address is in the same format as the LAN Configuration screen. An example of an address is: `C 192.007.007 001`

`IP network address`

The IP addresses of all the remote networks that can be reached through the gateway whose IP address is configured in the previous field. If the gateway node is to serve as a default gateway, enter an at sign (@) in one of these fields.

`IP mask`

The IP mask allows you to specify a subnet mask for each reachable network. This is in the same format as an IP address. This mask is optional.

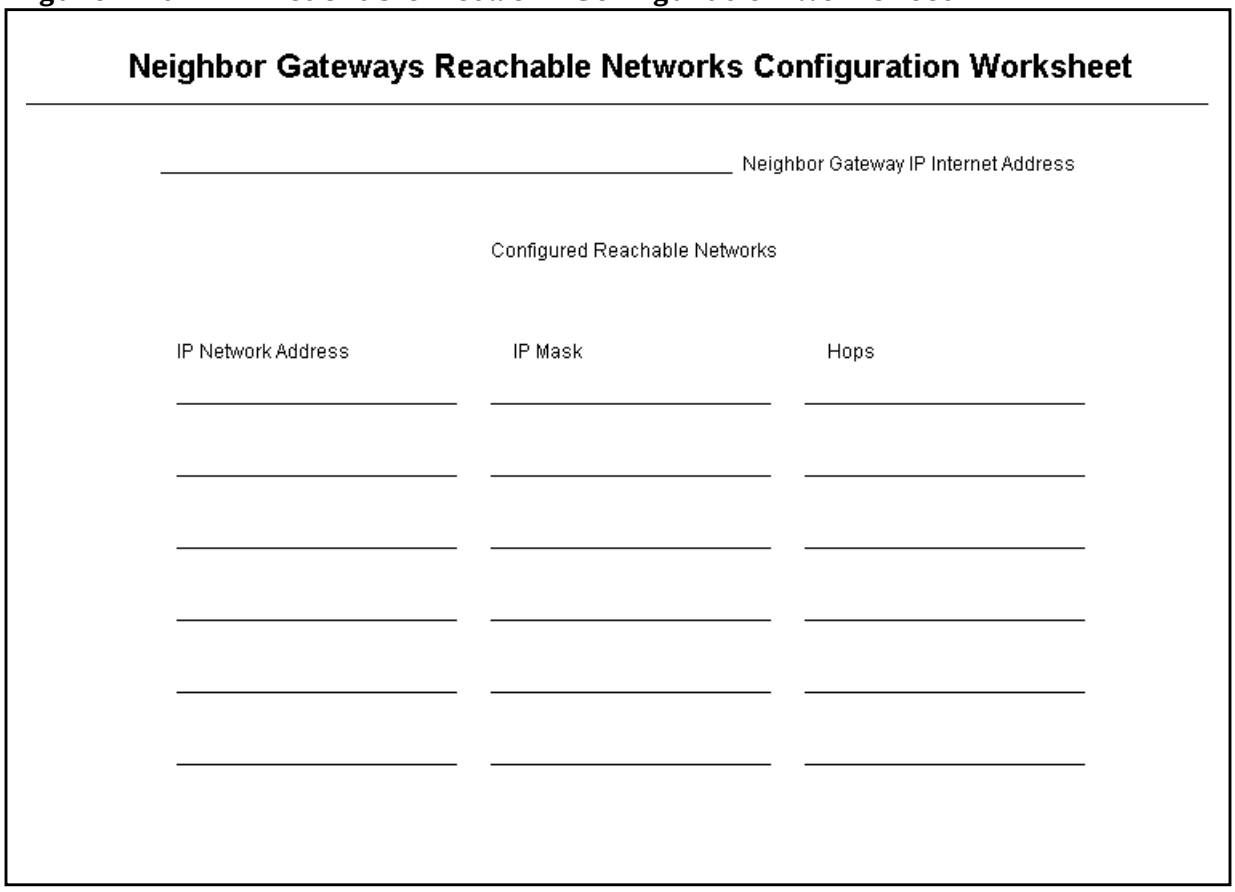
`Hops`

This is the number of hops (full gateways) that a packet travels to reach a remote network from a local network. Two partner gateway halves count as one hop.

Neighbor Gateway Reachable Networks Configuration Worksheet

Fill out the following worksheet (Figure 4-10) for each neighbor gateway reachable network you are configuring.

Figure 4-10 Reachable Network Configuration Worksheet

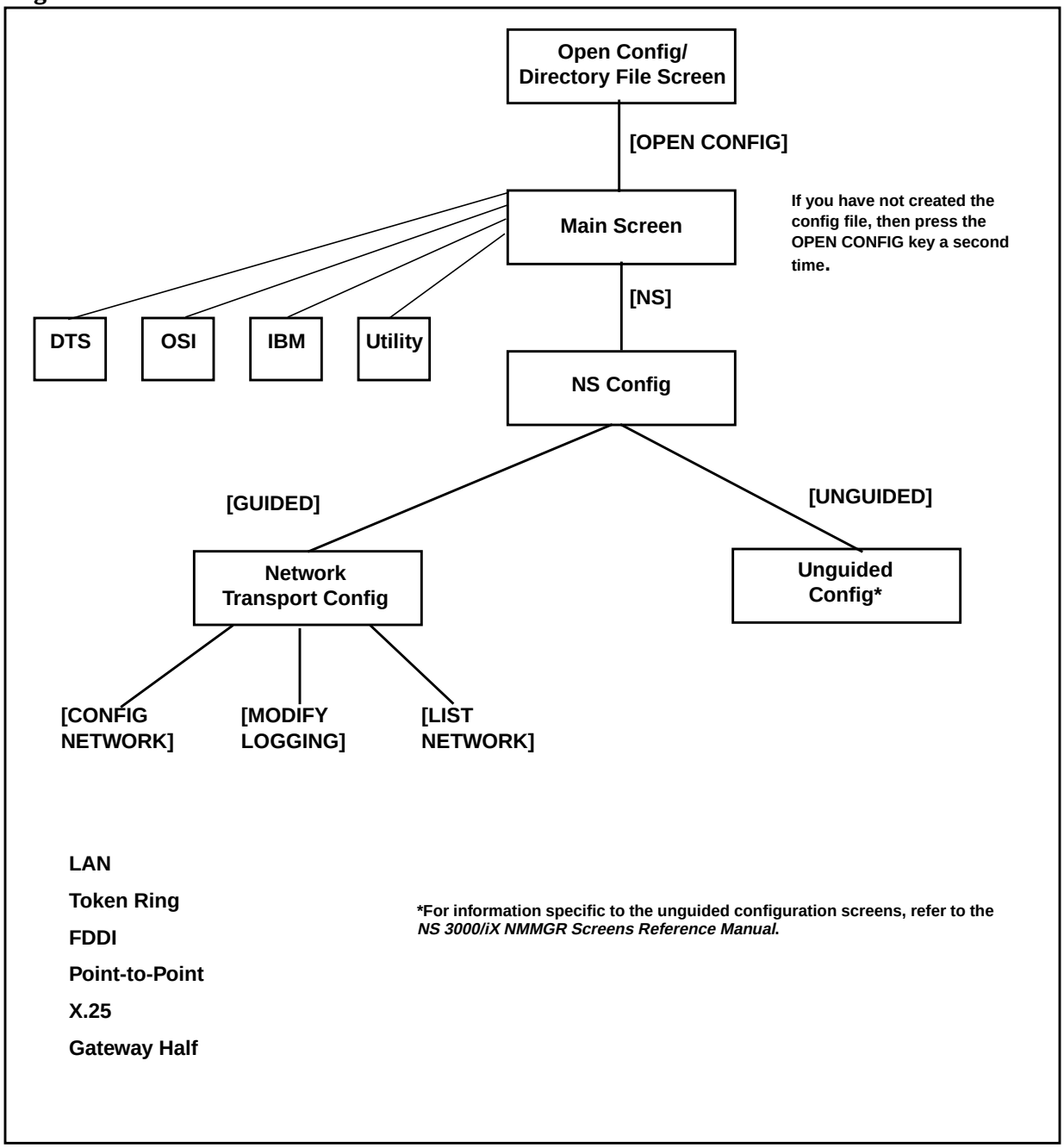


5 Introductory Screens

The introductory screens are the first few screens that are displayed when you configure a node using NMMGR.

Figure 5-1 shows the screen flow of the introductory screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow. This chapter describes the introductory screens relevant to configuring NS unguided networks.

Figure 5-1 NMMGR Screen Flow



Begin Configuration Process

The procedures that follow describe how to modify the NMMGR configuration file for the introductory screens.

Start NMMGR

Node manager (NM) or network administrator (NA) capabilities are required to run this program.

To run NMMGR:

1. Type `NMMGR.PUB.SYS` at the system prompt (`:`).
2. Press **[RETURN]**.

NOTE

You can modify the link configurations in `NMCONFIG.PUB.SYS` when the **Network Services** are active. However, the network must be stopped and restarted for the changes made in NMMGR to be implemented.

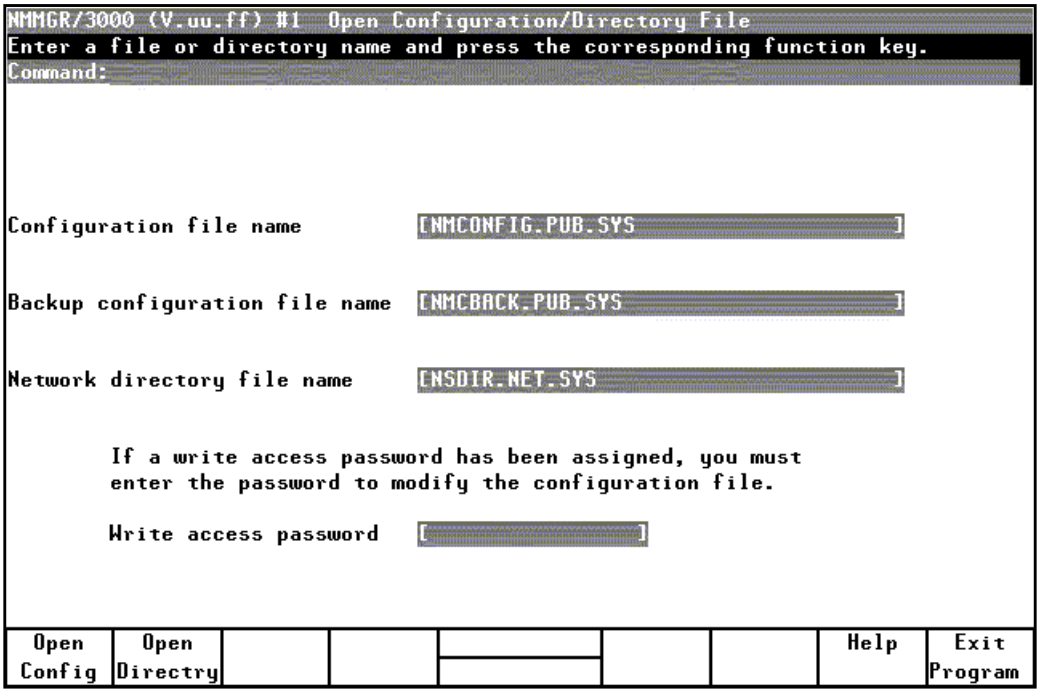
If NS is down, you will see the following two messages in response to the `NETCONTROL STATUS` command:

```
TRANSPORT NOT ACTIVE. (NETEXPORTWARN 0001) ENCOUNTERED ONE
OR MORE WARNINGS WHILE PROCESSING COMMAND. (CIWARN 4437)
```

Open Configuration File

The Open Configuration/Directory File screen (#1) in Figure 5-2 is the first screen displayed when you run NMMGR.

Figure 5-2 Open Configuration/Directory File Screen



Follow the steps listed here to enter data for this screen. Refer to "Fields" subsection for detailed information about each field on the screen.

Step 1. Verify that the correct configuration file name, backup configuration file name, and network directory file name are in the appropriate fields.

Step 2. If you have assigned a write access password, enter it in this field. If you are not using the password feature, leave this field blank.

Step 3. Press the **[Open Config]** key. If you are creating the configuration file for the first time, NMMGR will ask you to verify creation. Press the **[Open Config]** key again to continue.

Fields

`configuration file name`

The only configuration file name the system recognizes for use by the network subsystem is `NMCONFIG.PUB.SYS`. You can, however, create or modify a configuration file using a different name and save it as an offline configuration file. You can use offline configuration files as a means of creating and storing configurations that you want to use in the future or that you are preparing for use on a different system.

When you are ready to use an **offline configuration file**, rename it as NMCONFIG.PUB.SYS and reboot the system. (Keep in mind that any file you use as a configuration file must be successfully validated before you try to use it.)

`Backup configurationfile name`

A backup file name must be specified whenever a configuration file is opened or created. The default backup configuration file name is NMCBACK.group.account. The backup file will be automatically updated with the contents of the configuration file each time the configuration file is successfully validated.

`Network directory file name`

A network directory must be configured in the following circumstances:

- nodes running X.25
- nodes not using domain name services
- nodes on a LAN network that do not support the HP-PROBE protocol

The only network directory file name supported by HP is NSDIR.NET.SYS. This file is part of a KSAM pair. A key file is created at the same time as this data file. The key file will automatically be named using the first six letters of the network directory file name, appended with the character K. For example, NSDIRK.NET.SYS is the name of the key file associated with the data file NSDIR.NET.SYS. If the name of the data file is less than six letters long, then the entire file name would be appended with a K.

`Write access password`

The password is an optional feature. If a password has been assigned, you must enter it in the password field to update the configuration file or the directory file. It is still possible to open an existing file without using an assigned password, but the file will be in read only mode and NMMGR will not accept changes.

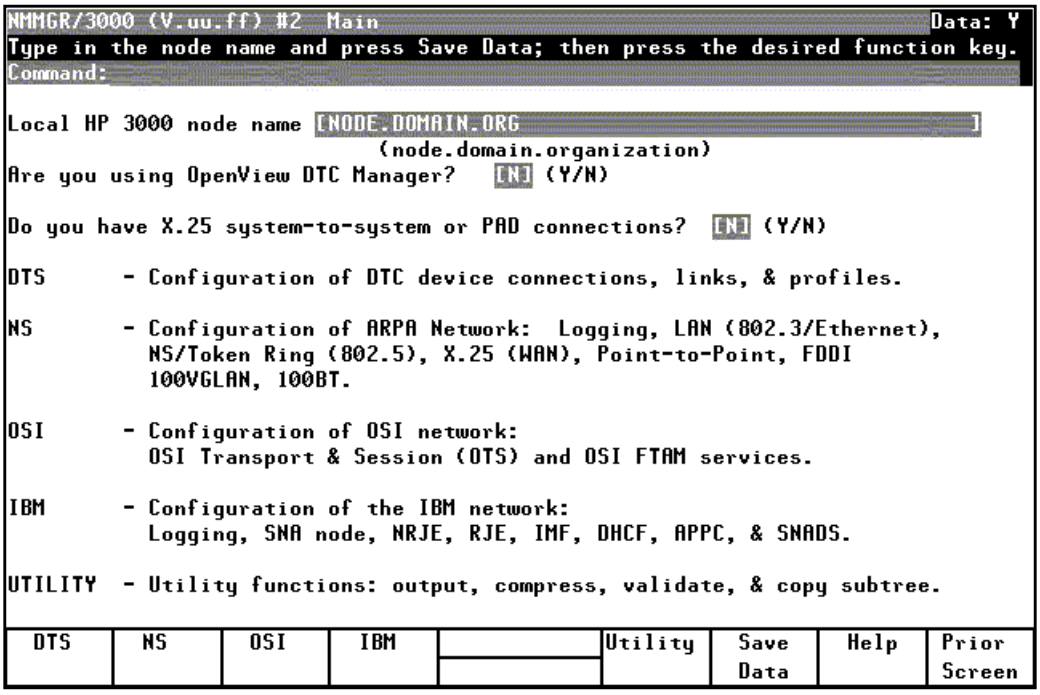
If a password has not been assigned, you should ignore the password field.

If you want to assign a password for the system you are configuring, see U*sing the Node Management Services (NMS) Utilities*.

Select NS Configuration

To Select NS Configuration. The Main screen (#2) in Figure 5-3 is displayed after you create or open a configuration file by pressing the **[Open Config]** key from the Open Configuration Directory File screen (#1) in Figure 5-2.

Figure 5-3 Main Screen



Step 1. Ensure that the information in the fields on this screen is correct. If not, or if the information has not been entered, specify the correct information and press the **[Save Data]** key. (See *Configuring Systems for Terminals, Printers, and Other Serial Devices* for information about configuring the information on this screen.)

Step 2. When you are satisfied with the information as configured, press the **[NS]** key to select the NS configuration branch.

Fields

`Local node name`

The local node name is the name by which the HP e3000 computer is known in the network. The format of a node name is nodename.domain.organization where the total number of characters is 50 or fewer, and each field contains 16 or fewer characters (alphanumeric, underscore, or hyphens). The first character of each field must be alphabetic.

The nodename portion of each node name must be unique within the node's network. The nodename.domain portion of each node name must be unique within the internetwork. HP recommends that all nodes on the network be assigned the same domain and organization.

Assign meaningful node names. For example, MKTG.BND.HP and LAB.BND.HP are meaningful names for two nodes on the same network within Hewlett-Packard. One node (MKTG.BND.HP) is used by the marketing department. The other node (LAB.BND.HP) is used by the lab. The domain field is the same because the nodes belong to the same network. The organization field is the same because the nodes belong to the same internetwork.

`Are you using OpenView DTC Manager?`

If you answer yes to this question, NMMGR assumes you are using a PC to manage your system and takes you to the corresponding set of screens when you configure DTS. If you answer no, NMMGR assumes you are using host-based network management and takes you to a different set of DTS screens. You should already have answered this question when you configured DTS.

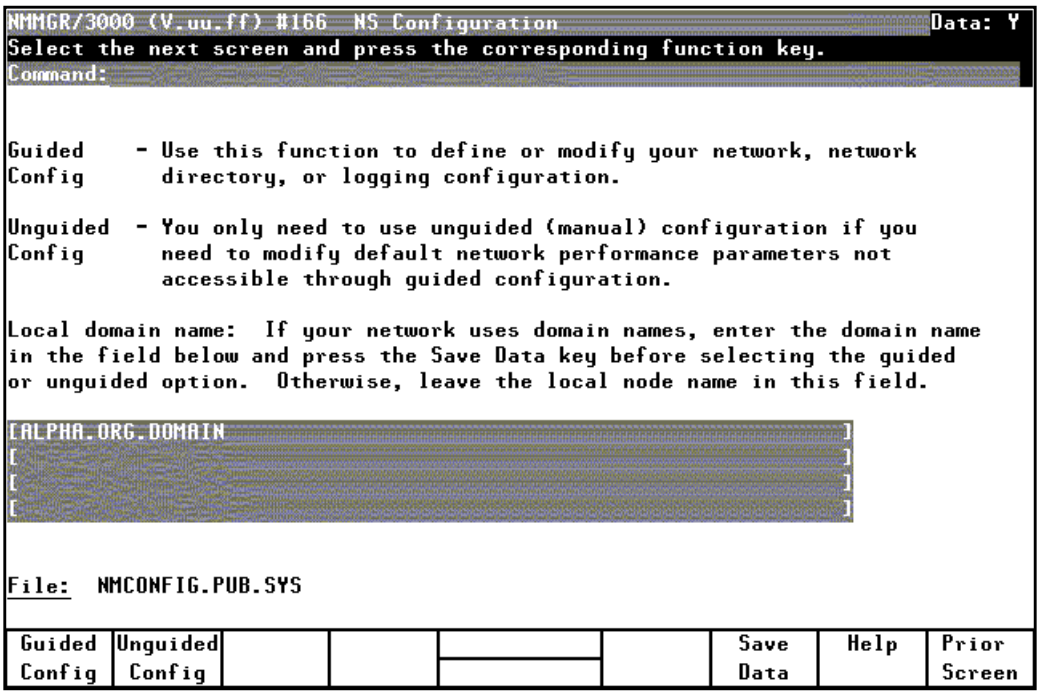
`Do you have X.25 system- to-system or PAD connections?`

If you answer yes to this question, NMMGR assumes you are configuring X.25 connections and takes you to the set of screens required to configure DTC X.25 Network Access Cards when you configure DTS. If you answer no, NMMGR assumes you have no need to configure X.25 connections and takes you to a different set of DTS screens. You should already have answered this question when you configured DTS.

Select Guided Configuration

The NS Configuration screen (#166) in Figure 5-4 is displayed if you press the **[NS]** key at the Main screen (#2) in Figure 5-3.

Figure 5-4 NS Configuration Screen



Step 1. If you are using domain names for network access, replace the node name in the field at the bottom of the screen with this system's domain name and press the **[Save Data]** key. If not using domain names, leave the node name as is.

Step 2. Press the **[Guided Config]** key to proceed with guided configuration of LAN.

Guided/Unguided Configuration

Hewlett-Packard recommends that you press the **[Guided Config]** key to select the guided configuration branch whenever you need to initially configure a network interface. Guided configuration supplies many default values for your configuration and requires that you visit a minimal number of screens. This manual provides information on every screen available to you through unguided NS configuration.

The **[Unguided Config]** key is used to modify configuration values that are not available in the guided screens. To use the unguided configuration screens, refer to the *NS 3000/iX NMMGR Screens Reference Manual*.

Fields

`Local Domain Name`

The name of this system in the ARPANET standard format. This name can be used by other nodes on the network to access this host.

The domain name is composed of labels, with each label separated by a period. Each label must start with a letter or digit, and have as interior characters only letters, digits, hyphens (-), or underbars (_). A domain name may have any number of labels, but its total length, including periods, is limited to 255 characters.

`label[.label][...]`

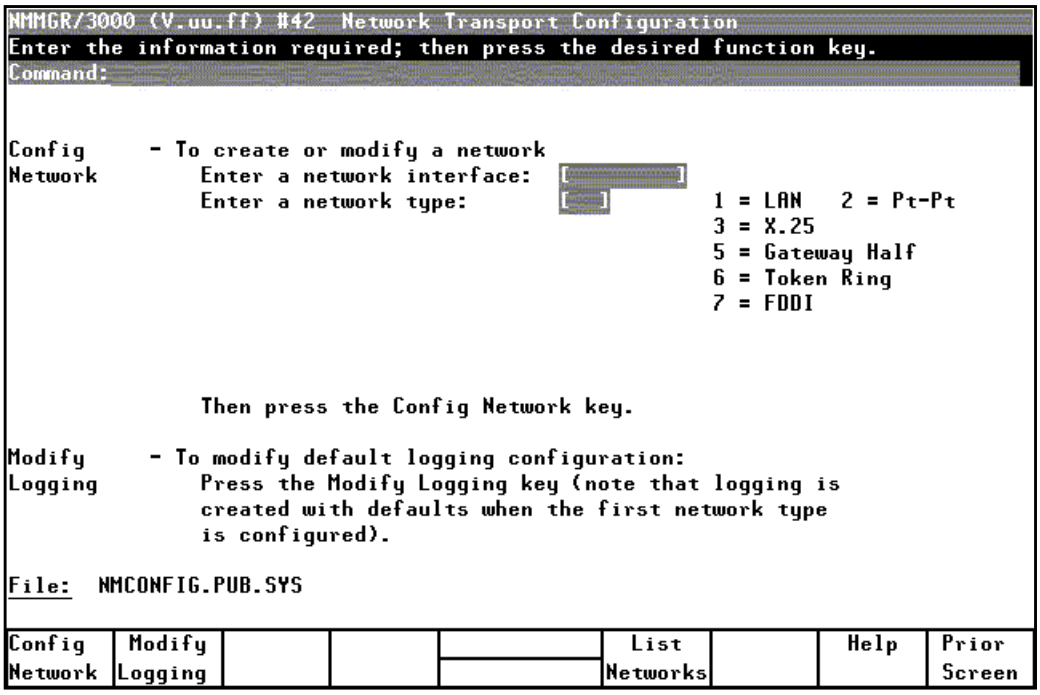
Domain names are not case sensitive.

Use of domain names is optional. If you are not using domain names for network access, leave the local node name in this field.

Perform Guided Network Transport Configuration

The Network Transport Configuration screen (#42) in Figure 5-5 is displayed if you press the **[Guided Config]** key at the NS Configuration screen (#166) in Figure 5-4.

Figure 5-5 Network Transport Configuration Screen



Step 1. Next to the words `Enter a network interface:`, enter a name for the selected network interface (for example, LANNI).

Step 2. Next to the words `Enter a network type:`, enter the selected network type number indicated on the above screen. (For example, enter a `1` to indicate that the NI is a LAN NI.)

Step 3. Press the **[Config Network]** key. (There may be a short pause before the next screen appears.)

Step 4. Proceed to the chapter of the network interface selected above for screen information. Refer to Chapter 6 , “Configuring a LAN Node,” for information on LAN, Token Ring, FDDI, 100VG-AnyLAN, and 100Base-T; and other chapters for information on Point-to-Point, X.25, and Gateway Half respectively.

Fields

`Enter a network interface`

The network name (NI name) is used to easily identify one of the types of network interfaces: LAN, Token Ring, FDDI, NS Point-to-Point, X.25 or Gateway Half. The name can be up to eight alphanumeric characters, starting with a letter. The maximum number of NIs that can be configured on a node is 48. **One of the 48 allowable NIs is reserved for loopback. (Loopback is configured for you automatically.)**

If a node interfaces to more than one network, give each NI on that node a unique name. Although all nodes on the same network do not have to have the same NI name, it will be easier to remember if you make the NI name the same for all nodes on the same network (for instance, `LANNET`). You will use the NI name with the `NETCONTROL` command to start the transport and network link.

`Enter a network type`

Number that indicates the type of network interface you are configuring. You must enter a network type if you are configuring a new network interface. Refer to the following for what number to enter:

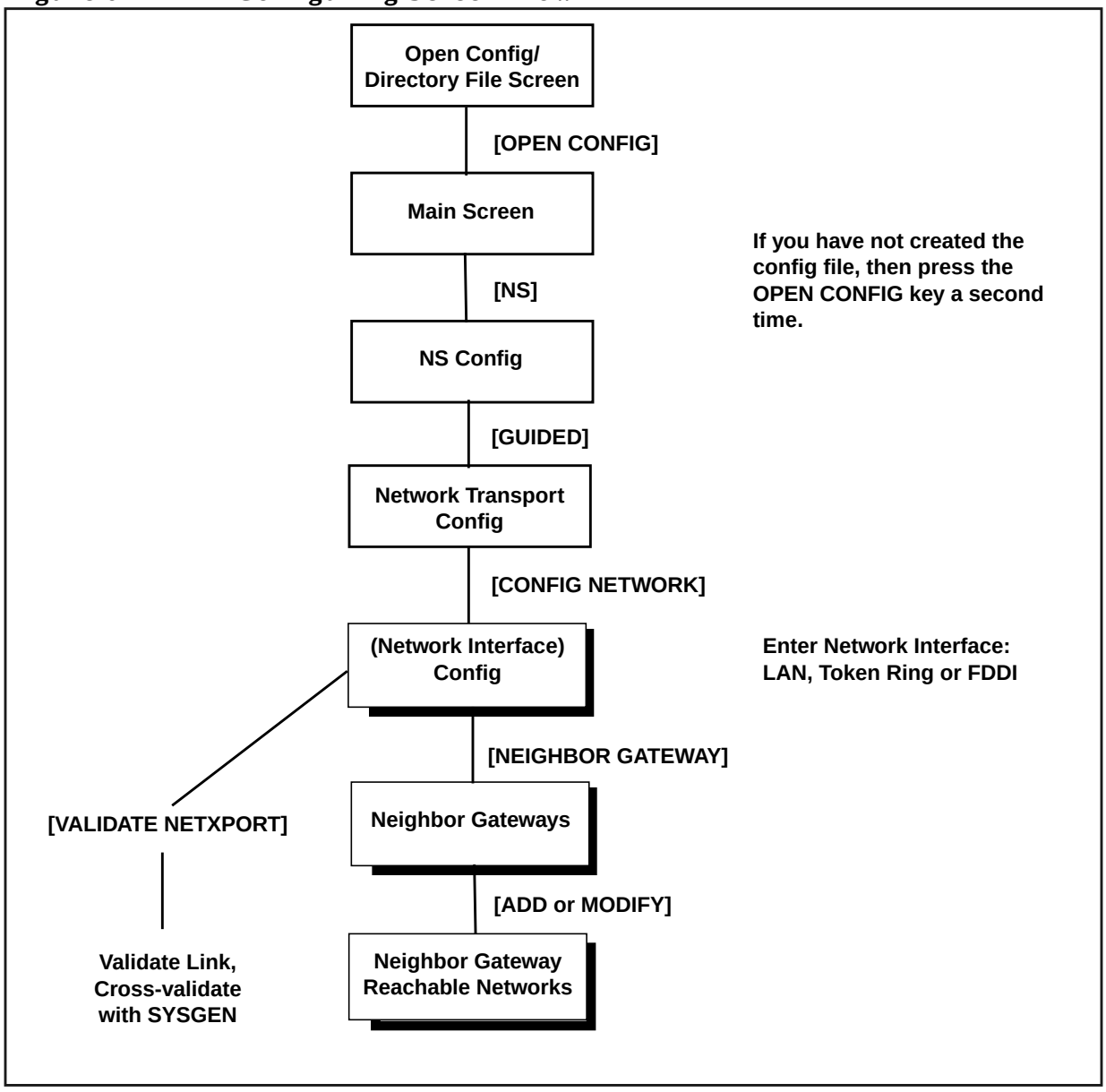
- Enter 1 for a LAN NI (100Base-T, ThinLAN or 100VG-AnyLAN)
- Enter 2 for a Point-to-Point (router) NI
- Enter 3 for an X.25 NI
- Enter 5 for a Gateway Half NI
- Enter 6 for a Token Ring NI
- Enter 7 for an FDDI NI

6 Configuring a LAN Node

This chapter provides step-by-step instructions for configuring local area network (LAN), Token Ring, Fiber Distributed Data Interface (FDDI), 100VG-AnyLAN, and 100Base-T links. This manual assumes that you are using the guided configuration capabilities of NMMGR.

Figure 6-1 shows the screen flow for configuring LAN, Token Ring, FDDI, 100VG-AnyLAN, and 100Base-T screens. Screens unique to the configuration of LAN, Token Ring, FDDI, 100VG-AnyLAN and 100Base-T are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 6-1 Configuring Screen Flow



Before using NMMGR to configure a link, you should complete the worksheets provided. See Chapter 4 , “Planning for Node Configuration,” for more information on planning your configuration and filling out the configuration worksheets.

This chapter includes step-by-step instructions to help you perform the following tasks:

- Begin the configuration process.
- Configure a LAN, Token Ring, FDDI, 100VG-AnyLAN, or 100Base-T network interface.

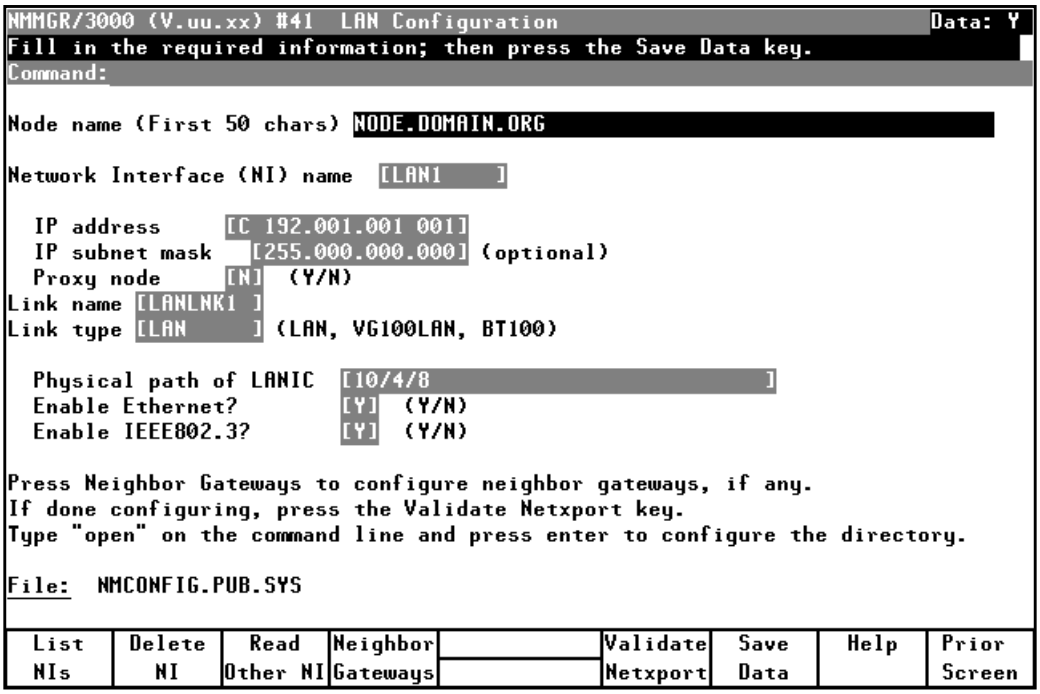
Once the above tasks are completed, refer to Chapter 10 , “Validating and Cross-Validating with SYSGEN,” for step-by-step instructions to help you perform the following validation tasks:

- Validate the network transport configuration.
- Cross-validate in SYSGEN.

Configure a LAN Network Interface

The LAN Configuration screen (#41) in Figure 6-2 is displayed when you press the **[Config Network]** key at the Network Transport Configuration screen (#42) with an NI type of 1 (LAN). Refer to Chapter 5 , "Introductory Screens," for information on the Network Transport Configuration screen.

Figure 6-2 LAN Configuration Screen



Step 1. In the IP address field, enter the internet protocol (IP) address for the node being configured. An example of an address is: C 192.191.191 009.

Step 2. The IP subnet mask is optional. If entering one, tab to the IP subnet mask field and enter the number in the same format as an IP address.

Step 3. The proxy node is optional. Enter Y only if your network has internetworks (networks with gateways) or non-HP nodes and you are not using domain name services.

Step 4. Move to the Link name field. Enter a link name to represent the LAN card for which you are configuring a link. This name must be unique to the node.

Step 5. Move to the Link type field. Enter BT100 for a 100Base-T link, LAN for a ThinLAN link, or VG100 LAN for a 100VG-AnyLAN link.

Step 6. Tab down to the field called `Physical path of LANIC`. Enter the physical path number corresponding to the SPU slot number where the LAN interface controller card is located.

Step 7. Tab down to the field called `Enable Ethernet (Y/N)`. By default, ethernet is enabled. Change the field to `N` if you *do not* want ethernet and the ARP protocol enabled.

Step 8. Tab down to field called `Enable IEEE 802.3 (Y/N)`. By default, IEEE 802.3 is enabled. Change the field to `N` if you *do not* want IEEE 802.3 and the Probe protocol enabled.

Step 9. Press the **[Save Data]** key to save the LAN link configuration. If you need to identify neighbor gateways, press the **[Neighbor Gateways]** key and proceed to the section in this chapter called "To Identify Neighbor Gateways." Otherwise, proceed to Chapter 10 , "Validating and Cross-Validating with SYSGEN," and press the **[Validate Netxport]** key.

`Optional Keys`

Press the **[List NIs]** key to list the names and types of already configured network interfaces.

Press the **[Delete NI]** key to remove a configured network interface from the configuration file.

Press the **[Read Other NI]** key to call up a previously configured Network Interface name.

Fields

`Node name`

Display only.

`Network Interface (NI) name`

Display only.

`IP address`

The IP address is an address of a node on a network. An IP address has two parts: a network portion and a node portion. The **network** portion must be the *same* for all nodes on a LAN network; the **node** portion must be *unique* for all nodes on a LAN network.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, `C 192.191.191 009`).

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between `0` and `255` separated by periods or blanks (for example, `15.123.44.98`).

You need not enter the following items as NMMGR will fill these in:

- Class A, B, C
- Leading zeros for the network and node portion of the IP address.

HP assigns the network portion (initial nine digits) of IP addresses from ARPA Class C, though your addresses may also be of Classes A or B. The complete formats are:

Class `A nnn xxx.xxx.xxx`

`B nnn.nnn xxx.xxx`

`C nnn.nnn.nnn xxx`

Where: `nnn` = the network portion of the IP address and
`xxx` = the node portion of the IP address.

For Class C, the `node` portion of the IP address must be between `001` and `254`.

If you are adding your NS 3000/iX node to an existing network, the network portion of each node's IP address should be the same. You will have to find out what this is, and use it in the network portion of the IP address of your NS 3000/iX node. Also, you will need to know the node portions of the IP addresses of each of the nodes (usually they will be numbered sequentially, such as `001`, `002`, and so on), so that you can specify a unique node portion for the IP address of your node. If you have a network map, it should provide a record of such items as the node name and IP address of each node. If there is no record, and if you want to find out each node's IP address, you will have to issue the following command (NM capability required) on each of the nodes:

```
NETCONTROL NET=NIname;STATUS
```

One of the lines of output from this command tells you what the complete IP address is for that node; the last three digits are the unique node portion of the class C address.

`IP subnet mask` — An IP subnet mask is specified in the same format as an IP address. The 32-bit mask is grouped in octets expressed as decimal integers and delimited by either a period (.) or a space. An IP mask is used when configuring subnetworks. The mask identifies which bits of an IP address will be used to define a subnetwork. To determine these bits, you first need to estimate how many subnetworks and nodes per subnetwork you need. See Chapter 2 , "Networking Concepts," for details on deriving an IP subnet mask.

`Proxy node`	Establishing a proxy node is a way of placing node name and address mapping information in a single location. If you are configuring an internetwork or a network with non-HP nodes, it may be easier to update your configurations if you have them located in a central place, that is, the proxy node. On an internetwork, the proxy node is usually a gateway. (It is not necessary to configure a proxy node if you have configured domain names. See Chapter 12 , “Configuring Domain Name Files,” for information on domain names.)
`Link name`	The link name can have up to eight alphanumeric characters and the first character must be alphabetic.
`Physical Path of LANIC`	The physical path number corresponds to the slot location of a node’s local area network interface controller (LANIC) card. Recommended slot locations and physical path calculations vary according to the type of HP e3000 system you are running. For the various platforms, physical path syntax (examples only) look like: Series 9x7: 48 Series 9x8: 56/44 Series 9x9: 10/4/16 Series 99x: 0/28/12 Series N4000: 1/10/0/0 Series A500: 0/2/0/0 If you are unsure of the slot location or of the physical path number to configure for your system, run the offline ODE MAPPER utility, see your system documentation, or consult your Hewlett-Packard service representative.

`Enable Ethernet?`

A `Y` in this field enables ethernet for the LAN. You can enable either ethernet or IEEE 802.3 or both simultaneously. One or the other must be enabled (both fields may not be set to `N`). Ethernet is enabled by default.

Disabling Ethernet has the effect of disabling the ARP protocol and you will need to handle both name to IP and IP to station (MAC) address resolution by other means.

`Enable IEEE 802.3?`

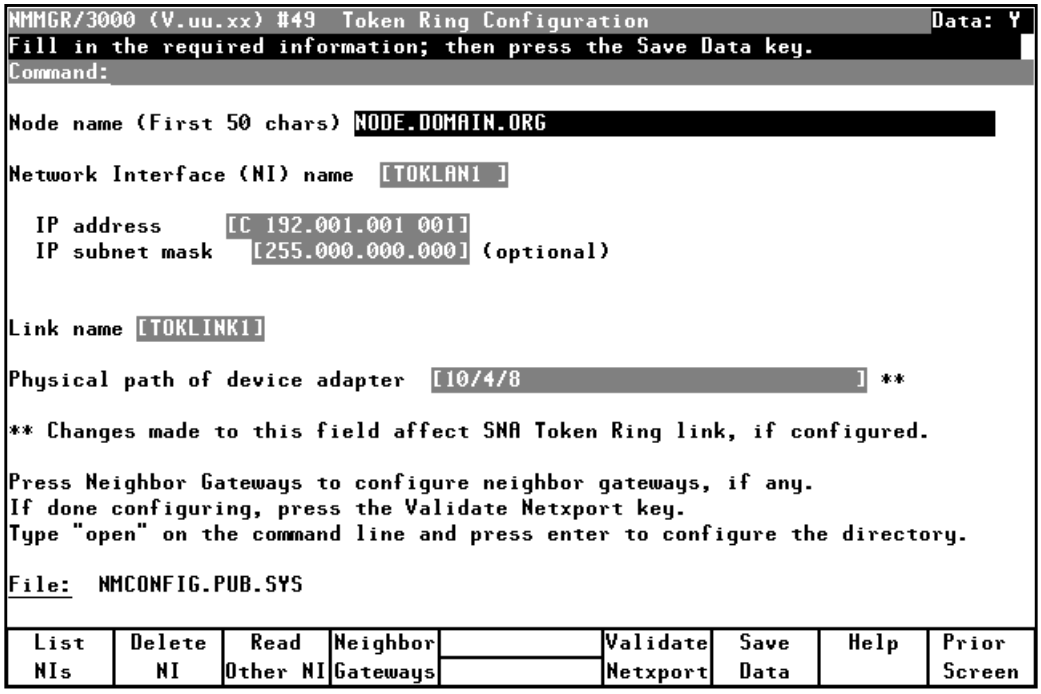
A `Y` in this field enables IEEE 802.3 for the LAN. You can enable either IEEE 802.3 or ethernet or both simultaneously. One or the other must be enabled (both fields may not be set to `N`). IEEE 802.3 is enabled by default.

Disabling IEEE 802.3 has the effect of disabling the probe protocol and you will need to handle both name to IP and IP to station (MAC) address resolution by other means.

Configure a Token Ring Network Interface

The Token Ring Configuration screen (#49) in Figure 6-3 is displayed when you press the **[Config Network]** key at the Network Transport Configuration screen (#42) with an NI type of 6 (Token Ring). Refer to Chapter 5 , “Introductory Screens,” for information on the Network Transport Configuration screen.

Figure 6-3 Token Ring Configuration Screen



Step 1. In the `IP address` field, enter the internet protocol (IP) address for the node being configured. An example of an address is `C 192.191.191 009`.

Step 2. The IP subnet mask is optional. If entering one, tab to the `IP subnet mask` field and enter the number in the same format as an IP address.

Step 3. Move to the `Link name` field. Enter a link name to represent the Token Ring card for which you are configuring a link. This name must be unique to the node.

Step 4. Tab down to the field called `Physical Path of Token Ring Device Adapter`. Enter the physical path number corresponding to the SPU slot number where the Token Ring device adapter is located.

NOTE If the same Token Ring card is being used for both NS and SNA communications, you must use the same value for this field as is configured for the SNA Link.

Step 5. Press the **[Save Data]** key to save the Token Ring link configuration. If you need to identify neighbor gateways, press the **[Neighbor Gateways]** key and proceed to the section in the chapter called "To Identify Neighbor Gateways." Otherwise, proceed to Chapter 10 , "Validating and Cross-Validating with SYSGEN," and press the **[Validate Netxport]** key.

`Optional Keys` Press the **[List NIs]** key to list the names and types of already configured network interfaces.

Press the **[Delete NI]** key to remove a configured network interface from the configuration file.

Press the **[Read Other NI]** key to call up a previously configured Network Interface name.

Fields

`Node name`

Display only.

`Network Interface (NI) name`

Display only.

`IP address`

The IP address is an address of a node on a network. An IP address has two parts: a network portion and a node portion. The **network** portion must be the *same* for all nodes on a LAN network; the **node** portion must be *unique* for all nodes on a LAN network.

`Class` `A nnn xxx.xxx.xxx`

`B nnn.nnn xxx.xxx`

`C nnn.nnn.nnn xxx`

Where: `nnn` = the network portion of the IP address and `xxx` = the node portion of the IP address.

For Class C, the `node` portion of the IP address must be between `001` and `254`.

If you are adding your NS 3000/iX node to an existing network, the network portion of each node's IP address should be the same. You will have to find out what this is, and use it in the network portion of the IP address of your NS 3000/iX node. Also, you will need to know the node portions of the IP addresses of each of the nodes (usually they will be numbered sequentially, such as `001`, `002`, and so on), so that you can specify a unique node portion for the IP address of your node. If you have a network map, it should provide a record of such items as the node name and IP address of each node. If there is no record, and if you want to find out each node's IP address, you will have to issue the following command (NM capability required) on each of the nodes:

```
NETCONTROL NET=NIname;STATUS
```

One of the lines of output from this command tells you what the complete IP address is for that node; the last three digits are the unique node portion of the class C address.

`IP subnet mask`

An IP subnet mask is specified in the same format as an IP address. The 32-bit mask is grouped in octets expressed as decimal integers and delimited by either a period (.) or a space. An IP mask is used when configuring subnetworks. The mask identifies which bits of the IP address comprise the network and subnetwork portion.

`Link name`

The link name can have up to eight alphanumeric characters and the first character must be alphabetic.

NOTE If the same Token Ring card is being used for both NS and SNA communications, you must use the same name in this field as is configured for the SNA Link.

`Physical path of device adapter`

The physical path number corresponds to the slot location of a node's device adapter. Recommended slot locations and physical path calculations vary according to the type of HP e3000 system you are running.

If you are unsure of the slot location or of the physical path number to configure for your system, see your system documentation or consult your Hewlett-Packard service representative.

For the various platforms, physical path syntax (examples only) look like:

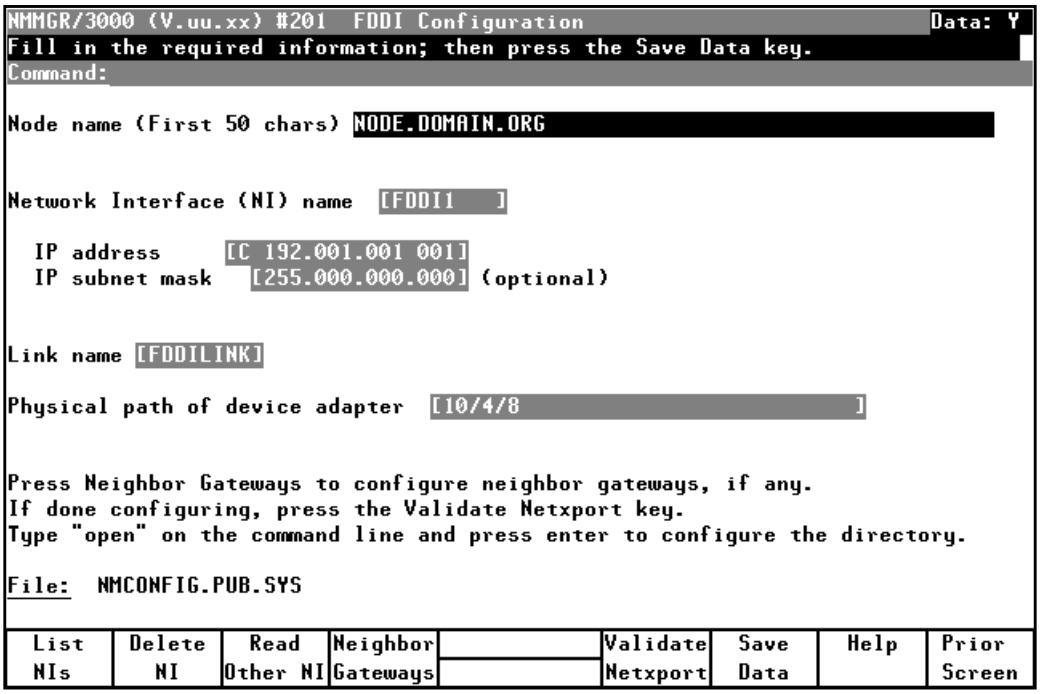
Series 9x7:	48
Series 9x8:	56/44
Series 9x9:	10/4/16
Series 99x:	0/28/12

If you are unsure of the slot location or of the physical path number to configure for your system, run the offline ODE MAPPER utility, see your system documentation, or consult your Hewlett-Packard service representative.

Configure an FDDI Network Interface

The FDDI Configuration screen (#201) in Figure 6-4 is displayed when you press the **[Config Network]** key at the Network Transport Configuration screen (#42) with an NI type of 7 (FDDI). Refer to Chapter 5 , “Introductory Screens,” for information on the Network Transport Configuration screen.

Figure 6-4 FDDI Configuration Screen



Step 1. In the `IP address` field, enter the internet protocol (IP) address for the node being configured. An example of an address is `C 192.191.191 009`.

Step 2. The IP subnet mask is optional. If entering one, tab to the `IP subnet mask` field and enter the number in the same format as an IP address.

Step 3. Move to the `Link name` field. Enter a link name to represent the FDDI card for which you are configuring a link. This name must be unique to the node.

Step 4. Tab down to the field called `Physical Path of FDDI Device Adapter`. Enter the physical path number corresponding to the SPU slot number where the FDDI device adapter is located.

Step 5. Press the **[Save Data]** key to save the FDDI link configuration. If you need to identify neighbor gateways, press the **[Neighbor Gateways]** key and proceed to the section in the chapter called "To Identify Neighbor Gateways." Otherwise, proceed to Chapter 10 , "Validating and Cross-Validating with SYSGEN," and press the **[Validate Netxport]** key.

`Optional Keys`

Press the **[List NIs]** key to list the names and types of already configured network interfaces.

Press the **[Delete NI]** key to remove a configured network interface from the configuration file.

Press the **[Read Other NI]** key to call up a previously configured Network Interface name.

Fields

`Node name`

Display only.

`Network Interface (NI) name`

Display only.

`IP address`

The IP address is an address of a node on a network. An IP address has two parts: a network portion and a node portion. The **network** portion must be the *same* for all nodes on a FDDI network; the **node** portion must be *unique* for all nodes on a FDDI network.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, `C 192.191.191 009`).

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, `15.123.44.98`).

   You need not enter the following items as NMMGR will fill these in:

   - Class A, B, C
   - Leading zeros for the network and node portion of the IP address.

HP assigns the network portion (initial nine digits) of IP addresses from ARPA Class C, though your addresses may also be of Classes A or B. The complete formats are:

```
Class   A nnn xxx.xxx.xxx
        B nnn.nnn xxx.xxx
        C nnn.nnn.nnn xxx
```

Where: nnn = the network portion of the IP address and
xxx = the node portion of the IP address.

For Class C, the node portion of the IP address must be between 001 and 254.

If you are adding your NS 3000/iX node to an existing network, the network portion of each node's IP address should be the same. You will have to find out what this is, and use it in the network portion of the IP address of your NS 3000/iX node. Also, you will need to know the node portions of the IP addresses of each of the nodes (usually they will be numbered sequentially, such as 001, 002, and so on), so that you can specify a unique node portion for the IP address of your node. If you have a network map, it should provide a record of such items as the node name and IP address of each node. If there is no record, and if you want to find out each node's IP address, you will have to issue the following command (NM capability required) on each of the nodes:

```
NETCONTROL NET=NIname;STATUS
```

One of the lines of output from this command tells you what the complete IP address is for that node; the last three digits are the unique node portion of the class C address.

`IP subnet mask`

An IP subnet mask is specified in the same format as an IP address. The 32-bit mask is grouped in octets expressed as decimal integers and delimited by either a period (.) or a space. An IP mask is used when configuring subnetworks. The mask identifies which bits of the IP address comprise the network and subnetwork portion.

`Link name`

The link name can have up to eight alphanumeric characters and the first character must be alphabetic.

`Physical path of device adapter`

The physical path number corresponds to the slot location of a node's FDDI device adapter. Recommended slot locations and physical path calculations vary

according to the type of HP e3000 system you are running.

For the various platforms, physical path syntax (examples only) look like:

Series 9x7:	48
Series 9x8:	56/44
Series 9x9:	10/4/16
Series 99x:	0/28/12

If you are unsure of the slot location or of the physical path number to configure for your system, run the offline ODE MAPPER utility, see your system documentation, or consult your Hewlett-Packard service representative.

Configure Neighbor Gateways

You need to visit the next two screens only if you are configuring a non-gateway node that is on the same network as a gateway. In this case, the non-gateway node needs to know the identity of any **neighbor gateway**. Neighbor gateways can be either full or half gateways.

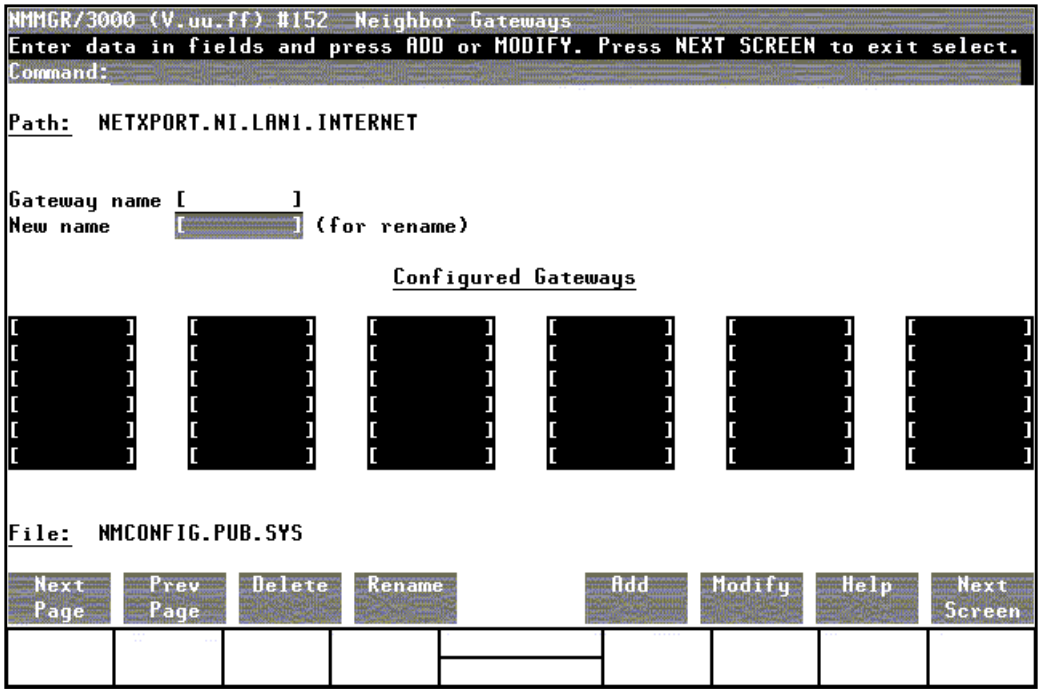
Gateways that are on the same network are called **neighbor gateways**. A non-gateway node on a LAN, Token Ring, or FDDI network may need to go through a neighbor gateway in order to send messages to an entirely different network. (Two nodes are on the same network if the **network** portion of their IP addresses are the same.) All LAN, Token Ring, FDDI, 100VG-AnyLAN or 100Base-T nodes that are on the same network as a neighbor gateway need to know the identity of any neighbor gateways. When you configure a LAN, Token Ring, FDDI, 100VG-AnyLAN, or 100Base-T node, you enter into its configuration the identity of any accessible neighbor gateways that share the same network. The identified gateways may be either full or half gateways.

You may designate gateways as **default gateways**. Messages for a network will be routed to a default gateway if there is no gateway configured for the destination network. The default gateway will then attempt to locate the destination of the message.

Identify Neighbor Gateways (If Any Are Present)

The Neighbor Gateways screen (#152) in Figure 6-5 is displayed when you press the **[Neighbor Gateways]** key at the selected Guided configuration screen for the LAN, Token Ring and FDDI networks.

Figure 6-5 Neighbor Gateways Screen



Step 1. In the `Gateway name` field, enter the name of a gateway that is on the *same network* as the node that you are configuring. (Nodes are on the same network if the network portions of their IP addresses are the same.).

Step 2. If you are adding the identified gateway for the first time, press the **[Add]** key. If you are modifying the configuration of this node, press the **[Modify]** key. The Neighbor Gateway Reachable Networks screen will be displayed. Proceed to "Identify Neighbor Gateway Reachable Networks.

Step 3. Repeat steps 1 and 2 for each gateway that is on the same network as the node that you are configuring. When you have finished, press the **[Next Screen]** key to return to the selected configuration screen (LAN, Token Ring, or FDDI) and proceed to Chapter 10 , "Validating and Cross-Validating with SYSGEN."

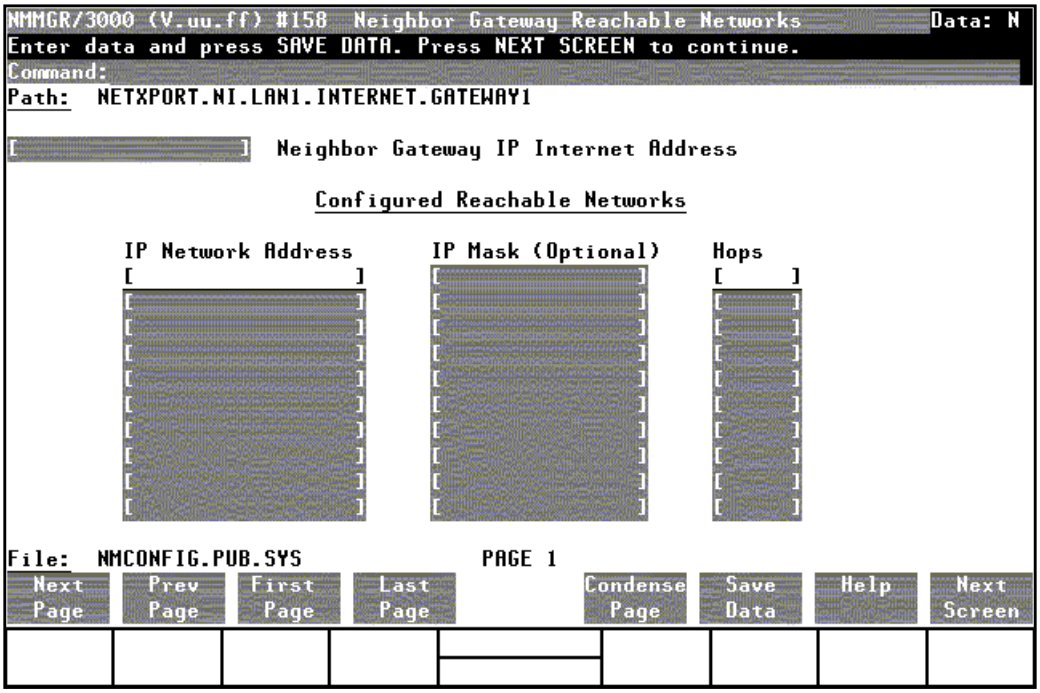
Fields

`Gateway name` Each gateway name can be as long as eight alphanumeric characters. The first character must be alphabetic.

Identify Neighbor Gateway Reachable Networks

The Neighbor Gateway Reachable Networks screen (#158) in Figure 6-6 is displayed when you press the **[Add]** or **[Modify]** key for a valid gateway name from the Neighbor Gateways screen (#152) in Figure 6-5.

Figure 6-6 Neighbor Gateway Reachable Networks Screen



Step 1. In the `Neighbor Gateway IP Internet Address` field, enter the IP address of the gateway specified on the Neighbor Gateways screen. `C 192.191.191 009` is a typical address.

Step 2. In the `IP Network Address` fields under the title `Configured Reachable Networks`, enter the IP addresses of all the *remote* networks that can be reached through the gateway whose IP address is configured in the previous field. If you want to designate this gateway as a default gateway, enter an at sign (@) in one of the fields as well.

Step 3. The IP subnet mask is optional. If entering one, tab to the next field. In the IP `subnet mask` field, enter the number in the same format as an IP address.

Step 4. In the field labeled `Hops`, enter the number of hops (full gateways) needed to get to the target network. Two partner gateway halves count as one hop.

Step 5. Repeat steps 2, 3, and 4 for each remote reachable network. **The information configured in this screen can extend to more than one page, if necessary, to allow configuration of up to 2550 reachable networks per link (255 pages and 10 reachable nets**

per page). If you need to configure more than 10 networks, press the **[Save Data]** key then press the **[Next Page]** key to enter more networks.

Step 6. After you have finished entering the IP addresses of all the reachable networks, press the **[Save Data]** key. Press the **[Prior Screen]** key to return to the Neighbor Gateways screen.

Step 7. Back at the Neighbor Gateways screen, after you have finished adding all of the neighboring gateways, press the **[Prior Screen]** key to return to the selected configuration screen (LAN, Token Ring, or FDDI). Proceed to Chapter 10 , "Validating and Cross-Validating with SYSGEN."

Fields

If you have identified any neighbor gateways, then you will also be identifying: 1) the *IP Network Addresses* of all of the networks that you can reach through that gateway, and 2) the *number of hops* (corresponding to the number of gateways) that a packet passes through to reach a remote network from the local network. Two gateway halves count as one hop.

`Neighbor Gateway IP Internet Address`

The IP address of the gateway whose name you have specified on the Neighbor Gateways Screen. The IP address is in the same format as the selected configuration screen (LAN, Token Ring, or FDDI).

`IP Network Address`

In the fields under this heading, you list the IP addresses of all of the networks that you will be able to reach through the gateway you are configuring. **You also use this field to indicate whether or not the gateway is to serve as a default gateway by entering an at sign (@) to specify that it is a default gateway. Only one gateway can be designated as a default gateway for each HP e3000 system**.

`IP Mask (Optional)`

The fields under this heading allow you to specify a subnet mask for each reachable network. This mask is optional.

`Hops`

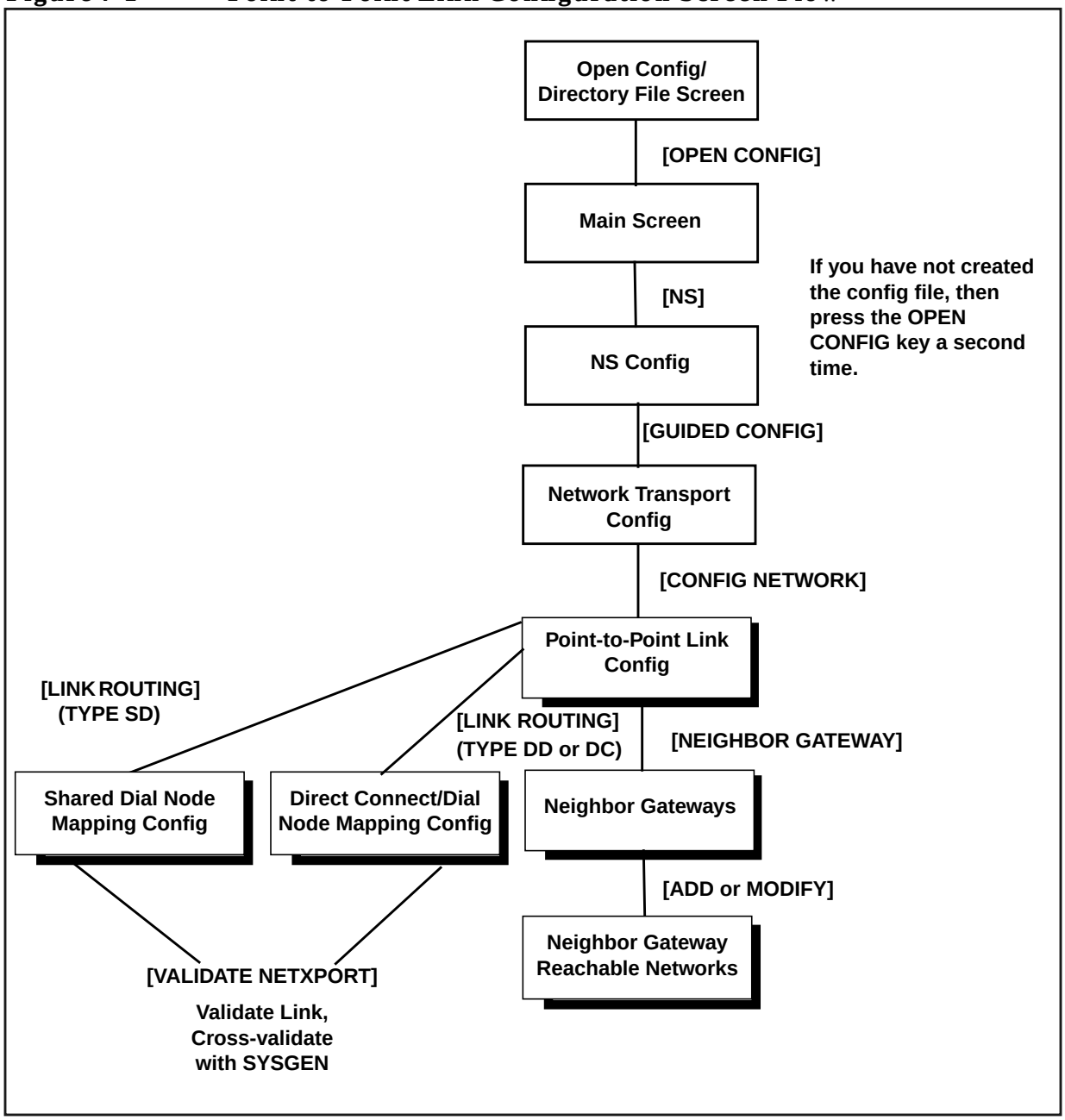
In the fields under this heading, enter the number of hops corresponding to the number of gateways that a packet travels to reach a remote network from a local network.

7 Configuring a Point-to-Point Node

This chapter provides step-by-step instructions for configuring Point-to-Point links. (Point-to-Point links are sometimes referred to as **router** links.) This manual assumes that you are using the guided configuration capabilities of NMMGR.

Figure 7-1 shows the screen flow for configuring Point-to-Point screens. Screens unique to Point-to-Point configuration are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 7-1 Point-to-Point Link Configuration Screen Flow



Before using NMMGR to configure a link, you should complete the worksheets provided. See Chapter 4 , “Planning for Node Configuration,” for more information on planning your configuration and filling out the configuration worksheets.

This chapter includes step-by-step instructions to help you perform the following tasks:

- Begin the configuration process.
- Configure a Point-to-Point network interface.
- Configure neighbor gateways.
- Configure node mapping.

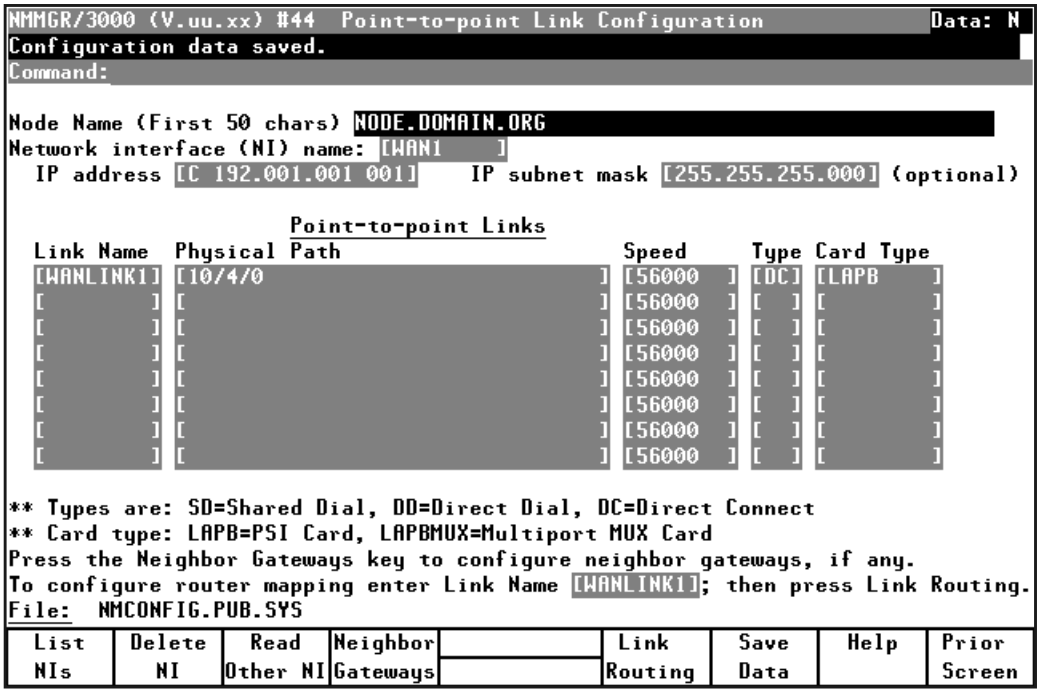
Once the above tasks are completed, refer to Chapter 10 , “Validating and Cross-Validating with SYSGEN,” for step-by-step instructions to help you perform the following validation tasks:

- Validate the network transport configuration.
- Cross-validate in SYSGEN.

Configure a Point-to-Point Network Interface

The Point-to-Point Configuration screen (#44) in Figure 7-2 is displayed when you press the **[Config Network]** key at the Network Transport Configuration screen (#42) with an NI type of 2 (Point-to-Point). Refer Chapter 5 , “Introductory Screens,” for information on the Network Transport Configuration screen.

Figure 7-2 Point-to-Point Link Configuration Screen



Step 1. In the `IP address` field, enter the internet protocol (IP) address for the node being configured. An example of an address is:
`C 192.191.191 009`.

Step 2. The IP subnet mask is optional. If entering one, tab to the `IP subnet mask` field and enter the number in the same format as an IP address.

Step 3. Move to the `Link Name` field. Enter a link name to represent the Point-to-Point card for which you are configuring a link. This name must be unique to both the node and the network interface (NI). **Up to 40 network links are supported per Point-to-Point (router) NI. (Up to eight network links are supported per screen. To configure additional links, save the current screen and then clear the screen to add additional links.)**

Step 4. Tab down to the `Physical Path` field. Enter the physical path number corresponding to the SPU slot number of the programmable serial interface (PSI) card, or slot and part of advanced communication controller (ACC) card.

Step 5. Tab to the Speed field. Enter the line transmission speed of this link.

Step 6. Tab to the Type field. Enter DD for direct dial, SD for shared dial or DC for direct connection.

Step 7. Tab to the Card Type field. Enter LAPBMUX if ACC adapter is being used, or LAPB for a PSI adapter. Do not mix both Card Types under the same NI.

Step 8. Press the **[Save Data]** key to record the data you have entered.

Step 9. If you need to identify neighbor gateways, press the [**Neighbor Gateways]** key and proceed to the section in this chapter called "To Configure Neighbor Gateways."

Step 10. If you have already configured neighbor gateways for this link or your network contains no neighbor gateways, press the **[Link Routing]** key and proceed to the section in this chapter titled "To Configure Node Mapping."

Optional Keys Press the **[List NIs]** key to list the names and types of already configured network interfaces.

Press the **[Delete NI]** key to remove a configured network interface from the configuration file.

Press the **[Read Other NI]** key to call up a previously configured Network Interface name.

There are two methods of entering an internet protocol (IP) address within NMMGR:

Fields

Node name

Display only.

Network Interface (NI) name

Display only.

IP address

The IP address is an address of a node on a network. An IP address has two parts: a network portion and a node portion. The **network** portion must be the *same* for all nodes on a LAN network; the **node** portion must be *unique* for all nodes on a LAN network.

1. Enter the fully qualified IP address (for example, Class C, C 192.191.191 009).

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between 0 and 255 separated by periods or blanks (for example, 15.123.44.98).

You need not enter the following items as NMMGR will fill these in:

- Class A, B, C
- Leading zeros for the network and node portion of the IP address.

HP assigns the network portion (initial nine digits) of IP addresses from ARPA Class C, though your addresses may also be of Classes A or B. The complete formats are:

```
Class   A nnn xxx.xxx.xxx
        B nnn.nnn xxx.xxx
        C nnn.nnn.nnn xxx
```

Where: nnn = the network portion of the IP address and
xxx = the node portion of the IP address.

For Class C, the node portion of the IP address must be between 001 and 254.

If you are adding your NS 3000/iX node to an existing network, the network portion of each node's IP address should be the same. You will have to find out what this is, and use it in the network portion of the IP address of your NS 3000/iX node. Also, you will need to know the node portions of the IP addresses of each of the nodes (usually they will be numbered sequentially, such as 001, 002, and so on), so that you can specify a unique node portion for the IP address of your node. If you have a network map, it should provide a record of such items as the node name and IP address of each node. If there is no record, and if you want to find out each node's IP address, you will have to issue the following command (NM capability required) on each of the nodes:

```
NETCONTROL NET=NIname;STATUS
```

One of the lines of output from this command tells you what the complete IP address is for that node; the last three digits are the unique node portion of the class C address.

Card Type	Specify LAPB if the adapter card used for this link is a single port PSI adapter. Specify LAPBMUX if this link is using one port on a multi-port synchronous MUX adapter card (ACC). Note: Card types cannot be mixed on the same NI.
IP subnet mask	An IP subnet mask is specified in the same format as an IP address. The 32-bit mask is grouped in octets expressed as decimal integers and delimited by either a period (.) or a

space. An IP mask is used when configuring subnetworks. The mask identifies which bits of an IP address will be used to define a subnetwork. To determine these bits, you first need to estimate how many subnetworks and nodes per subnetwork you need. See Chapter 2 , “Networking Concepts,” for details on deriving an IP subnet mask.

`Link Name`

The link name can have up to eight alphanumeric characters and the first character must be alphabetic.

`Physical Path`

The physical path number corresponds to the slot location of a node's programmable serial interface (PSI) card, and LAPBMUX card (ACC). Recommended slot locations and physical path calculations vary according to the type of HP e3000 system you are running.

For the various platforms, physical path syntax (examples only) look like:

Series 9x7:	48
Series 9x8:	56/44
Series 9x9:	10/4/16
Series 99x:	0/28/12
Series N4000:	1/10/0/1.7
Series A500:	0/2/0/1.4

If you are unsure of the slot location or of the physical path number to configure for your system, run the offline ODE MAPPER utility, see your system documentation, or consult your Hewlett-Packard service representative.

`Speed`

The line transmission speed is given in bits per second. For direct connect the value, must be supported by the cable. Values are 1200, 2400, 4800, 9600, 19200, 38400, 56000, and 64000. The default is 56000.

Type	Enter DD (direct dial) if you always want to call the same host over a dial link. If you choose DD the remote host does not have to be adjacent and other nodes can be accessed through the remote host. Enter SD if you want to call more than one adjacent remote node over a dial link without reconfiguring. If you choose SD, no other remote nodes can be accessed through the remote host; it is an end point in the connection. Enter DC if the link is a leased line, private line, or other non-switched link.

Configure Neighbor Gateways

You need to visit the next two screens only if you are configuring a non-gateway node that is on the same network as a gateway. In this case, the non-gateway node needs to know the identity of any **neighbor gateway**. Neighbor gateways can be either full or half gateways.

Gateways that are on the same network are called **neighbor gateways**. A non-gateway node on a Point-to-Point network may need to go through a neighbor gateway in order to send messages to an entirely different network. (Two nodes are on the same network if the **network** portion of their IP addresses are the same.) All Point-to-Point nodes that are on the same network as a neighbor gateway need to know the identity of any neighbor gateways. When you configure a Point-to-Point node, you enter into its configuration the identity of any accessible neighbor gateways that share the same network. The identified gateways may be either full or half gateways.

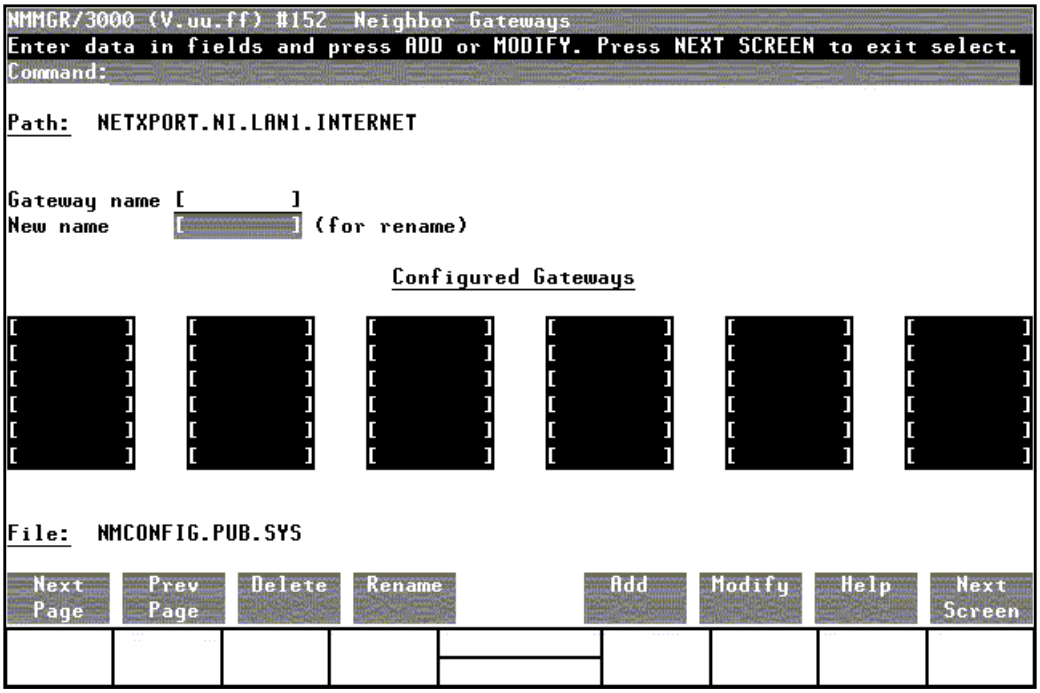
You may designate one gateway as a **default gateway**. Messages for a network will be routed to the default gateway if there is no gateway configured for the destination network. The default gateway will then attempt to locate the destination of the message.

NOTE HP e3000 should not be used as a gateway.

Specify Neighbor Gateways (If Any Are Present)

The Neighbor Gateways screen (#152) in Figure 7-3 is displayed when you press the **[Neighbor Gateways]** key at the Point-to-Point Link Configuration screen (#44) in Figure 7-2.

Figure 7-3 Neighbor Gateway Screen



Step 1. In the `Gateway name` field, enter the name of a gateway that is on the *same network* as the node that you are configuring. (Nodes are on the same network if the network portions of their IP addresses are the same.).

Step 2. If you are adding the identified gateway for the first time, press the **[Add]** key. If you are modifying the configuration of this node, press the **[Modify]** key. The Neighbor Gateway Reachable Networks screen will be displayed. Proceed to the section in this chapter titled "To Identify Neighbor Gateway Reachable Networks."

Step 3. Repeat steps 1 and 2 for each gateway that is on the same network as the node that you are configuring. When you have finished, press the **[Prior Screen]** key to return to the Point-to-Point Configuration screen and proceed to the section in this chapter titled "To Configure Node Mapping."

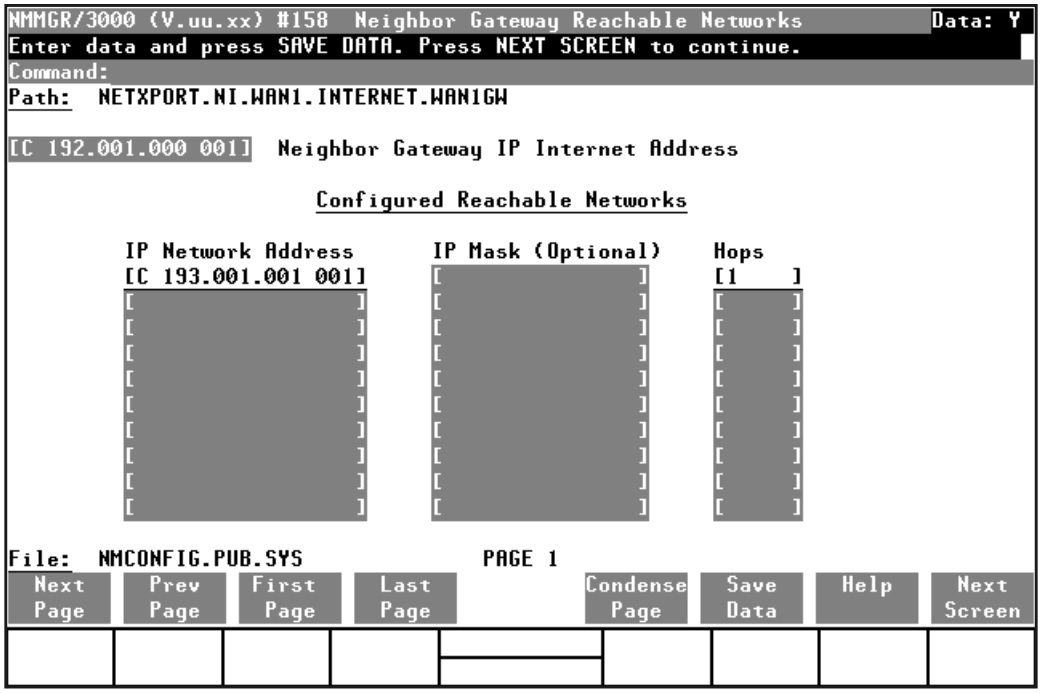
Fields

`Gateway name` Each gateway name can be as long as eight alphanumeric characters. The first character must be alphabetic.

Specify Neighbor Gateway Reachable Networks

The Neighbor Gateway Reachable Networks screen (#158) in figure 7-4 is displayed when you press the **[Add]** key or the **[Modify]** key for a valid gateway name from the Neighbor Gateways screen (#152) in Figure 7-3.

Figure 7-4 Neighbor Gateway Reachable Networks



Step 1. In the `Neighbor Gateway IP Internet Address` field, enter the IP address of the gateway specified on the Neighbor Gateways screen. An example of an address is: `C 192.191.191 009`.

Step 2. In the `IP Network Address` fields under the title `Configured Reachable Networks`, enter the IP addresses of all the *remote* networks that can be reached through the gateway whose IP address is configured in the previous field.

Step 3. The IP subnet mask is optional. If entering one, tab to the next field. In the IP `subnet mask` field, enter the number in the same format as an IP address.

Step 4. In the field labeled `Hops`, enter the number of hops (full gateways) needed to get to the target network. Two partner gateway halves count as one hop.

Step 5. Repeat steps 2, 3, and 4 for each remote reachable network. **The information configured in this screen can extend to more than one page, if necessary, to allow configuration of up to 2550 reachable networks per link (255 pages and 10 reachable nets per page)**. If you need to configure more than 10 networks, press the **[Save Data]** key then press the **[Next Page]** key to enter more networks.

Step 6. After you have finished entering the IP addresses of all the reachable networks, press the **[Save Data]** key. Press the **[Prior Screen]** key to return to the Neighbor Gateways screen.

Step 7. Back at the Neighbor Gateways screen, after you have finished adding all of the neighboring gateways, press the **[Prior Screen]** key to return to the Point-to-Point Link Configuration screen. Proceed to the section in this chapter titled "To Configure Node Mapping."

Fields

If you have identified any neighbor gateways, then you will also be identifying: 1) the *IP Network Addresses* of all of the networks that you can reach through that gateway, and 2) the *number of hops* (corresponding to the number of gateways) that a packet passes through to reach a remote network from the local network. Two gateway halves count as one hop.

`Neighbor Gateway IP Internet Address`

The IP address of the gateway whose name you have specified on the Neighbor Gateways Screen. The IP address is in the same format as on the Point-to-Point Configuration screen.

`IP Network Address`

In the fields under this heading, you list the IP addresses of all of the networks that you will be able to reach through the gateway you are configuring. **You also use this field to indicate whether or not the gateway is to serve as a default gateway by entering an at sign (@) to specify that it is a default gateway. Only one gateway can be designated as a default gateway for each HP e3000 system**.

`IP Mask (Optional)`

The fields under this heading allow you to specify a subnet mask for each reachable network. This mask is optional. See Chapter 2 , "Networking Concepts," for details on deriving the IP mask.

`Hops`

In the fields under this heading, enter the number of hops corresponding to the number of gateways that a packet travels to reach a remote network from a local network. Note: if you choose SD, *no* other nodes can be accessed through the remote host; it is an end point in the connection. Enter DC if the link is a leased line, private line, or other non-switched link.

Configure Node Mapping

The screens discussed in the following pages allow you to configure shared dial or direct connect and dial node mapping. These screens allow you to specify routes to target (destination) nodes and to indicate the priority of each route.

The number of mappings you enter depends on how many links are on the node you are configuring.

Nodes Having Single Links

If you are configuring a node (call it Node A) that has only one Point-to-Point link to a second node (call it Node B), you enter one route name as the mapping to the adjacent node (Node B).

If there are additional nodes attainable beyond Node B, you would only have to enter one more mapping: make up a route name, and then you can indicate the additional (non-adjacent) nodes by specifying a "wildcard" (@) in the destination IP address field of either the Dialed or Non-dialed Node Mapping Configuration screens.

Nodes Having Multiple Links

If you are configuring a node that has more than one Point-to-Point link, you could ultimately have several paths to a *non-adjacent* destination node. Hence, if this node has more than one Point-to-Point link, enter a symbolic route name for every other destination node on the network.

The route name is only used during configuration of this node, and you do not have to repeat it when you configure other nodes.

Select a Node Mapping Screen

To begin configuring node mapping, you should be at the Point-to-Point Link Configuration screen (#44) in Figure 7-2. You will configure node mapping for each link you are configuring.

Step 1. Enter the name of a configured link in the field at the bottom of the screen next to the words `To configure router mapping enter Link Name`.

Step 2. Press the **[Link Routing]** key.

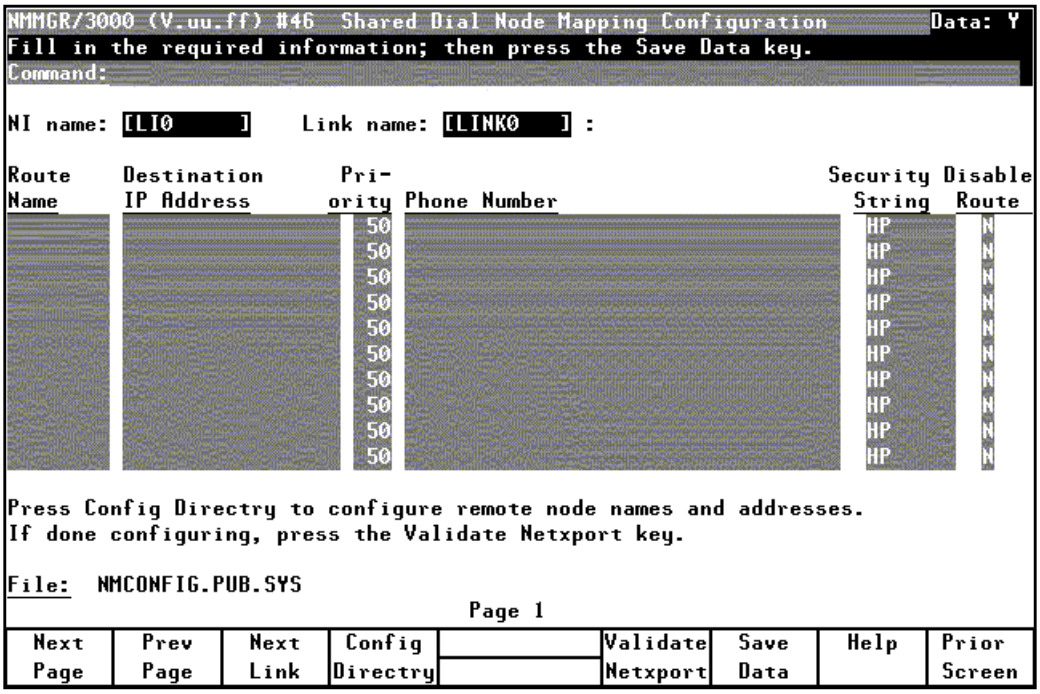
Step 3. If the Type specified for the selected link is `SD`, proceed to the section in this chapter titled "To Configure Shared Dial Node Mapping."

Step 4. If the Type specified for the selected link is `DD` or `DC`, proceed to the section in this section titled "To Configure Direct Connect/Dial Node Mapping."

Configure Shared Dial Node Mapping

The Shared Dial Node Mapping Configuration screen (#46) in Figure 7-5is displayed if you press the **[Link Routing]** key at the Point-to-Point Link Configuration screen (#44) for a link of type SD.

Figure 7-5 Shared Dial Node Mapping Configuration Screen



Each router NI can have up to 1024 mappings. However, 4096 is the absolute maximum number of unique phone numbers supported per NMCONFIG File.

Step 1. In the Route Name field, enter a symbolic name that represents a route between the node you are configuring and destination node

Step 2. In the Destination IP Address field, enter the IP address of the destination node for which a route is being specified.

Step 3. In the Priority field, enter a number from 1 to 99 to indicate the priority of this route if there are multiple routes to a destination.

Step 4. In the Phone Number field, enter the telephone number of the destination node. (Leave this field blank if the target node is non-adjacent.)

Step 5. The Security String field is optional. You may enter a string that remote nodes must use to gain dial link access to the node you are configuring.

Step 6. In the `Disable Route` field, leave the default alone unless you want to temporarily disable a configured route.

Step 7. Press the **[Save Data]** key to save the data on the screen. Proceed to Chapter 10 , "Validating and Cross-Validating with SYSGEN," and press the **[Validate Netxport]** key.

`Optional Keys`

Press the **[Next Link]** key to call up another link when you want to configure information about its adjacent and non-adjacent nodes.

Press the **[Config Directry]** key to configure the Network Directory screen.

Fields

`Route Name`

A symbolic name, up to eight alphanumeric characters, that represents a route between the node you are configuring and a destination node. The route name is only used within the NMMGR program. It is most useful when the node you are configuring has more than one possible way of accessing a target (destination) node. It identifies different routes to target nodes and is not the actual target node name. It is used because you may need a way to identify more than one route to a target node. There should be at lease one symbolic route name for routes to every other destination node on the network unless you use the "@" wildcard destination IP address.

To help keep track of routes, you can use the destination node name as the route name. If you have more than one route to a given node, you can name the routes *nodename*1, *nodename*2, and so forth.

`Destination IP Address`

IP address of the target (destination) node for which a route is being defined.

`Priority`

Number from 1 to 99 that indicates which route has precedence (priority) over another when there are multiple routes to a destination. A route to a destination that has a higher priority will take precedence over a route with a lower priority. This field is the primary means of influencing the choice of route.

`Phone Number`

Required if the link is a dial link. The field must be blank if the target node is non-adjacent. Enter the telephone number as a combination of decimal numbers (`0` through `9`), dashes, and the following special characters:

`/`	Separator used for automatic call units that have second dial-tone detect.
`E`	Optional end-of-number indicator.
`D`	Three-second delay (used for European modems and automatic call units that require built-in delays).
#	Defined by local phone system.
*	Defined by local phone system.

To disable outbound dialing, enter an exclamation point (`!`) by itself in the phone number field.

Each router NI can have up to 1024 mappings. However, 4096 is the absolute maximum number of unique phone numbers supported per `NMCONFIG` File.

`Security String`

An optional security string that remote nodes must use to gain dial link access to the node. It can be up to eight alphanumeric characters, left justified, with no embedded blanks. The first character must be alphabetic.

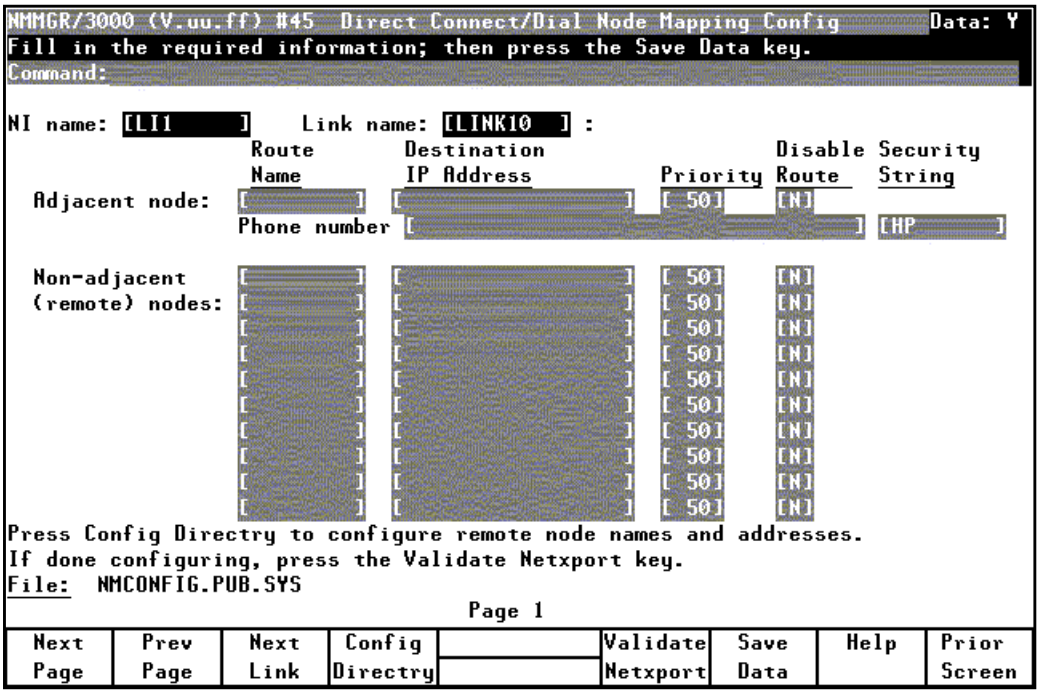
`Disable Route`

`Y` (yes) or `N` (no) indicator that allows you to temporarily disable a configured route. Leave the default (`N`) alone if you do not want to disable the route.

Configure Direct Connect/Dial Node Mapping

The Direct Connect/Dial Node Mapping Configuration screen (#45) in Figure 7-6 is displayed if you press the **[Link Routing]** key at the Point-to-Point Link Configuration screen (#44) for a link of type DD or DC.

Figure 7-6 Direct Connect/Dial Node Mapping Configuration Screen



Each router NI can have up to 1024 mappings. However, 4096 is the absolute maximum number of unique phone numbers supported per NMCONFIG File.

Step 1. In the Route Name field, enter a symbolic name that represents a route between the node you are configuring and a destination node.

Step 2. In the Destination IP Address field, enter the IP address of the destination node for which a route is being specified.

Step 3. In the Priority field, enter a number from 1 to 99 to indicate the priority of this route if there are multiple routes to a destination.

Step 4. In the Disable Route field, leave the default alone unless you want to temporarily disable a configured route.

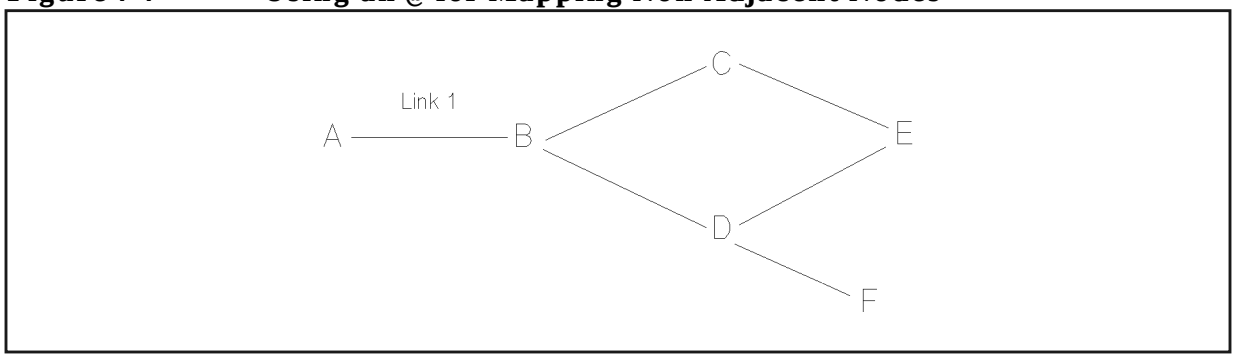
Step 5. If this is a dial link, in the Phone Number field, enter the telephone number of the destination node.

Step 6. The Security String field is optional. You may enter a string that remote nodes must use to gain dial link access to the node you are configuring.

Step 7. Enter information for non-adjacent (remote) nodes in the same manner in the fields provided. (You do not configure a phone number or security string for non-adjacent nodes.)

Step 8. Press the **[Save Data]** key to save the data on the screen. Proceed to Chapter 10 , "Validating and Cross-Validating with SYSGEN," and press the **[Validate Netxport]** key.

Figure 7-7 Using an @ for Mapping Non-Adjacent Nodes



`Priority`

Number from 1 to 99 that indicates which route has precedence (priority) over another when there are multiple routes to a destination. A route to a destination that has a higher priority will take precedence over a route with a lower priority.

`Disable Route`

`Y` (yes) or `N` (no) indicator that allows you to temporarily disable a configured route. Leave the default (`N`) alone if you do not want to disable the route.

`Phone Number`

Required if the link is a dial link. The field must be blank if the target node is non-adjacent. Enter the telephone number as a combination of decimal numbers (`0` through `9`), dashes, and the following special characters:

`/`	Separator used for automatic call units that have second dial-tone detect.
`E`	Optional end-of-number indicator.
`D`	Three-second delay (used for European modems and automatic call units that require built-in delays).
`#`	Defined by local phone system.
`*`	Defined by local phone system.

To disable outbound dialing, enter an exclamation point (!) by itself in the phone number field.

Each router NI can have up to 1024 mappings. However, 4096 is the absolute maximum number of unique phone numbers supported per NMCONFIG File.

`Security String`

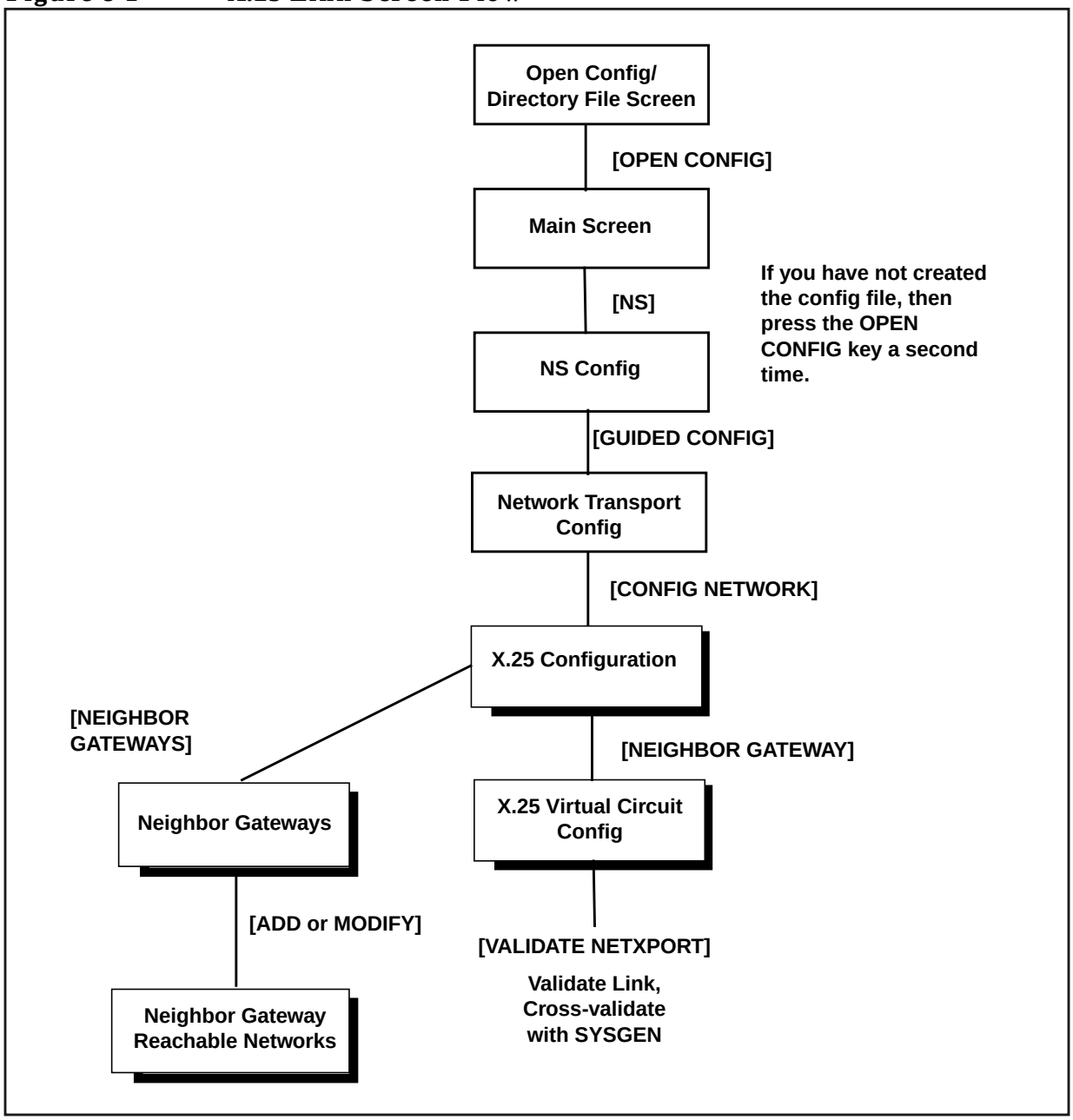
An optional security string that remote nodes must use to gain dial link access to the node. It can be up to eight alphanumeric characters, left justified, with no embedded blanks. The first character must be alphabetic.

8 Configuring a X.25 Node

This chapter provides step-by-step instructions for configuring X.25 iX System Access for systems using PC-based network management. This manual assumes that you are using the guided configuration capabilities of NMMGR.

Figure 8-1 shows the screen flow for configuring X.25 screens. Screens unique to X.25 configuration are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 8-1 X.25 Link Screen Flow



Before using NMMGR to configure a link, you should complete the worksheets provided. See Chapter 4 , “Planning for Node Configuration,” for more information on planning your configuration and filling out the configuration worksheets.

This chapter includes step-by-step instructions to help you perform the following tasks:

- Begin the configuration process.
- Configure an X.25 network interface.
- Configure neighbor gateways.

Once the above tasks are completed, refer to Chapter 10 , “Validating and Cross-Validating with SYSGEN,” for step-by-step instructions to help you perform the following validation tasks:

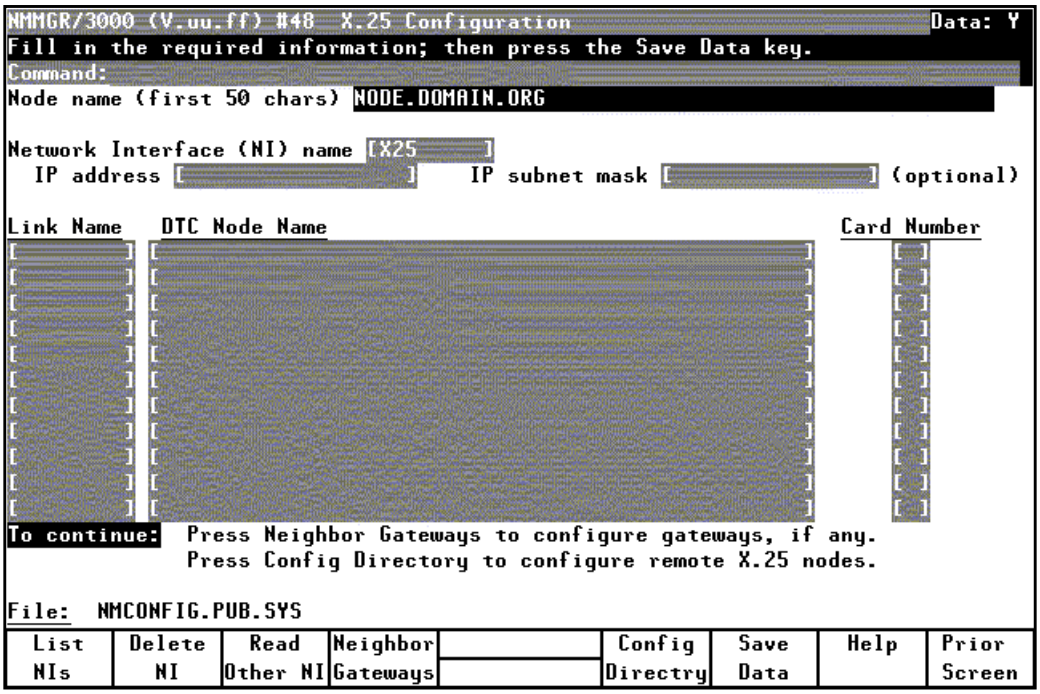
- Validate the network transport configuration.
- Cross-validate in SYSGEN.

NOTE If you are configuring X.25 iX System Access on a system that is using host-based network management (a PC running the HP OpenView Network Manager is not part of the network), use *Configuring and Managing Host-Based X.25 Links* instead of this manual for step-by-step configuration instructions.

Configure an X.25 Network Interface

The X.25 Configuration screen (#48) in Figure 8-2 is displayed when you press the **[Config Network]** key at the Network Transport Configuration screen (#42) with an NI type of 3 (X.25). Refer to Chapter 5 , “Introductory Screens,” for information on the Network Transport Configuration screen.

Figure 8-2 NS Configuration Screen



Step 1. In the `IP address` field, enter the internet protocol (IP) address for the node being configured. An example of an address is: `C 192.191.191 009`.

Step 2. The IP subnet mask is optional. If entering one, tab to the `IP subnet mask` field and enter the number in the same format as an IP address.

Step 3. Move to the first `Link name` field. Enter a link name to represent the DTC/X.25 Network Access card for which you are configuring a link. This name must be unique to both the node and the DTC. It must also be the same as the link name configured for this card when the Datacommunications and Terminal Subsystem (DTS) was configured.

Step 4. Enter the node name of the DTC that houses the DTC/X.25 Access card in the first `DTC Node Name` field then enter the slot number of the card in the `Card Number` field. Enter a link name, DTC node name, and card number for each link you are configuring.

Step 5. When you are done adding links, press the **[Save Data]** key.

Step 6. If the network that this node is on contains ANY internetwork gateway (either full or half) press the **[Neighbor Gateways]** key and proceed to the section in this chapter called "To Configure Neighbor Gateways."

Step 7. If the network that this node is on contains NO internetwork gateways or if you have already configured gateways for this system, press the **[Config Directry]** key and proceed to the section in this chapter titled "To Configure X.25 Virtual Circuits."

`Optional Keys` Press the **[List NIs]** key to list the names and types of already configured network interfaces.

Press the **[Delete NI]** key to remove a configured network interface from the configuration file.

Press the **[Read Other NI]** key to call up a previously configured Network Interface name.

Fields

`Node Name`

Display only.

`Network Interface (NI) name`

Display only.

`IP address`

IP address is an address of a node on a network. An IP address has two parts: a network portion and a node portion. The **network** portion must be the *same* for all nodes on an X.25 network; the **node** portion must be *unique* for all nodes on an X.25 network.

There are two methods of entering an internet protocol (IP) address within NMMGR:

1. Enter the fully qualified IP address (for example, Class C, `C 192.191.191 009`).

   OR

2. Enter only the network (*nnn*) and node (*xxx*) portions of the IP address as four positive integers between `0` and `255` separated by periods or blanks (for example, `15.123.44.98`).

   You need not enter the following items as NMMGR will fill these in:

   - Class A, B, C
   - Leading zeros for the network and node portion of the IP address.

HP assigns the network portion (initial nine digits) of IP addresses from ARPA Class C, though your addresses may also be of Classes A or B. The complete formats are:

```
Class   A nnn xxx.xxx.xxx
        B nnn.nnn xxx.xxx
        C nnn.nnn.nnn xxx
```

Where: nnn = the network portion of the IP address and xxx = the node portion of the IP address.

For Class C, the node portion of the IP address must be between 001 and 254.

If you are adding your NS 3000/iX node to an existing network, the network portion of each node's IP address should be the same. You will have to find out what this is, and use it in the network portion of the IP address of your NS 3000/iX node. Also, you will need to know the node portions of the IP addresses of each of the nodes (usually they will be numbered sequentially, such as 001, 002, and so on), so that you can specify a unique node portion for the IP address of your node. If you have a network map, it should provide a record of such items as the node name and IP address of each node. If there is no record, and if you want to find out each node's IP address, you will have to issue the following command (NM capability required) on each of the nodes:

```
NETCONTROL NET=NIname;STATUS
```

One of the lines of output from this command tells you what the complete IP address is for that node; the last three digits are the unique node portion of the class C address.

IP subnet mask

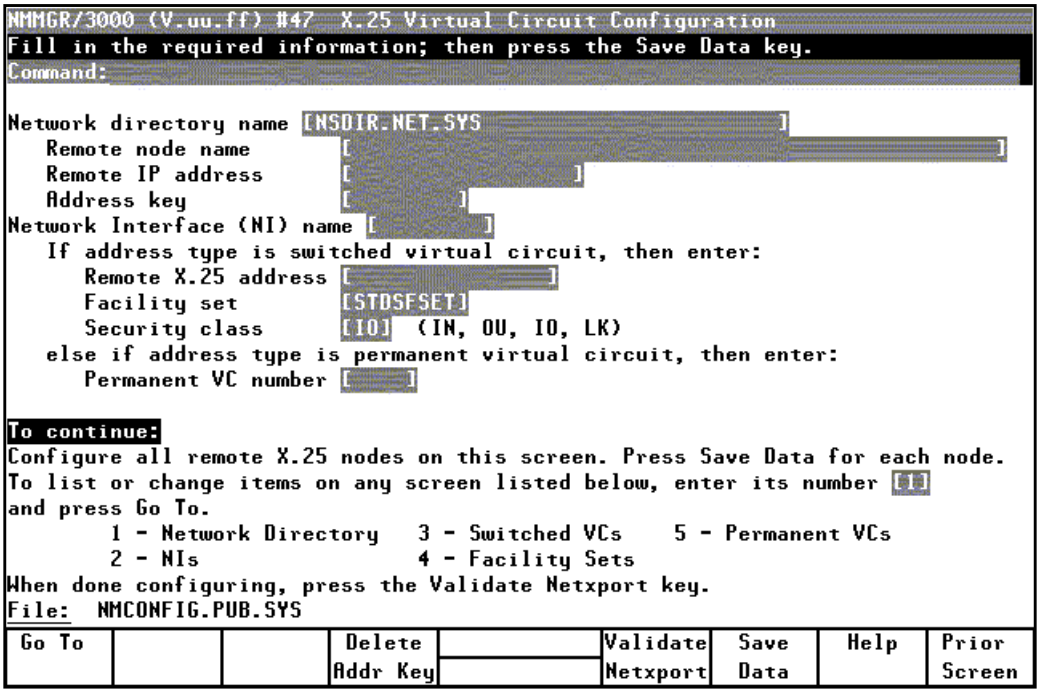
An IP subnet mask is specified in the same format as an IP address. The 32-bit mask is grouped in octets expressed as decimal integers and delimited by either a period (.) or a space. An IP mask is used when configuring subnetworks. The mask identifies which bits of an IP address will be used to define a subnetwork. To determine these bits, you first need to estimate how many subnetworks and

	nodes per subnetwork you need. See Chapter 2 , “Networking Concepts,” for details on deriving an IP subnet mask.
`Link Name`	The link name identifies a specific DTC/X.25 Network Access card to be used for X.25 system-to-system connections. This link name must be the same as the link name you entered for this card when you configured your DTCs. You may configure up to 11 links. (One link must be used for loopback. Loopback will be automatically configured during the guided screen configuration.)
`DTC Node Name`	The DTC node name is the fully qualified nodename (`name.domain.organization`) of the DTC that contains the DTC/X.25 Network Access card with the configured link name.
`Card Number`	The DTC card number is the number of the DTC/X.25 Network Access card in the associated DTC. If the card is contained in a DTC 48, the DTC card number can be any number from 1 to 5. If the card is contained in a DTC 16, the card number must be 2.

Configure X.25 Virtual Circuits

The X.25 Virtual Circuit Configuration screen (#47) in Figure 8-3 is displayed if you press the **[Config Directry]** key from the X.25 Configuration screen (#48) in Figure 8-2. This screen lets you configure the network directory.

Figure 8-3 X.25 Virtual Circuit Configuration Screen



Step 1. In the `Remote node name` field, type in the nodename of each remote X.25 node on your network in the format `nodename.domain.organization`. Also, if you need to be able to perform a loopback `DSLINE` command to the local node, then enter the local node's name here as well.

Step 2. For each node, type the IP address of the node in the `Remote IP address` field.

Step 3. To specify that calls can be made to a node, enter its address key in the `Address key` field. Enter the **node** portion of the remote node's configured nodename.

NOTE An address key called POOL is already preconfigured for you though it doesn't show up on the screen. POOL allows the node being configured to receive *any* incoming calls even if the remote system's address is not configured on this screen. POOL will also allow you to use NetIPC to programmatically provide an X.25 address that is not configured on this screen. If you want to delete the POOL address key, in the last line of the X.25 Virtual Circuit Configuration screen enter a 3 (for switched VCs) and press the **[Go To]** key. That brings you to the X.25 SVC Address Key Paths screen where you can then remove the default name POOL by typing over it with spaces and then saving the data.

Step 4. If the address type is a switched virtual circuit complete steps a through c, but if the address type is a permanent virtual circuit, skip to step 5.

a. In the Remote X.25 address field, enter the X.25 address of the remote host for X.25 public data networks or private networks.

b. Make sure the name of the facility set you are using is in the Facility set field. You may either choose the default facility set (STDSFSET) or enter an alternative. If you are configuring a new facility set, enter a new name. (To modify facility set parameters, enter a 5 in the last field on the screen and press the **[Go To]** key.)

c. In the Security class field, enter the level of logical security you want to have on this particular entry. The possible values are IN (accept calls from the address), IO (accept calls from and send calls to the address, default), OU (send calls to the address, incoming calls are rejected), and LK (block calls to or from the address).

Step 5. If the address type is a permanent virtual circuit (PVC), in the Permanent VC number field, enter the PVC number of the PVC on the remote node. This value cannot be greater than the number of PVCs for which you are subscribed. It must be within the PVC range you defined during DTC configuration.

Step 6. After you have finished entering new information for each remote node, press the **[Save Data]** key. (Press the key once for each remote node you are configuring.)

Step 7. If you have completed configuration of X.25, press the **[Validate Netxport]** key and proceed to Chapter 10 , "Validating and Cross-Validating with SYSGEN." Otherwise, press the **[Prior Screen]** key to return to the X.25 Configuration screen.

Fields

Network directory name

The network directory file that will be updated by the information entered through this screen.

`Remote node name`

You must enter the remote node name of each X.25 node into the network directory. Include entries for all remote nodes and, if you want to be able to perform loopback, the local node as well.

`Remote IP address`

Also in the network directory, you must enter the IP Address of each node whose identity you have entered into the network directory. For the format of this parameter, see the information in the "Fields" section under "Configure X.25 Network."

`Address key`

The X.25 address key is the name of a remote node with which your local node will be communicating. Hewlett-Packard recommends that you make the name be the node portion of the remote node's name (where its full name is `node.domain.organization`). You must configure an X.25 address key for each remote node with which your node will be communicating. You have a combined maximum of 1024 X.25 address keys in the SVC and PVC path tables. The X.25 address key name must be eight characters or less and the first character must be alphabetic. A default address key called `POOL` allows any system to access the local system even if the remote system's address is not configured. `POOL` can also be used when level 3 programmatic access (NetIPC) provides an X.25 address.

`Network Interface (NI) name`

Display only.

`SVC or PVC Parameters`

The parameters for assigning either SVCs or PVCs are described in the following paragraphs.

For SVCs

`Remote X.25 address`

The remote X.25 address is the remote node's X.25 address. This address is required for SVCs if you have specified an X.25 address key. This address must be 15 digits or less.

`Facility set`

The facility set name is a name for a set of X.25 connection parameters. The parameters are determined by the type of X.25 network that you are subscribed to. You can configure options in a facility set so that specified options are available for every virtual circuit or negotiated for each virtual circuit on a per-call basis. This facility set will be used when a connection is made from your node to the specified remote node or from the specified remote node to your node. A Facility Set is required for SVCs if you have specified an X.25 Address Key. The facility set name must be eight characters or less, and the first character must be alphabetic. You can configure up to 128 facility sets.

To modify facility set parameters, enter a `5` in the field at the bottom of the screen and press the **[Go To]** key. This will take you to the X.25 User Facility Sets screen. From this screen you can create new or modify existing user facility sets. See the *NS 3000/iX Screens Reference Manual* for more information.

`Security class`

The security class is the level of logical security you want to have when a connection is made to or from the specified remote node. A Security level is required for SVCs if you have specified an X.25 Address Key. The possible values are as follows:

- `IO` — Both incoming and outgoing calls are accepted. This is the default value.
- `IN` — Only incoming calls are accepted from this particular remote address. Outgoing calls will be rejected.
- `OU` — Only outgoing calls are accepted to this particular remote address. Incoming calls will be rejected.
- `LK` — Entry is locked. No call is accepted, either inbound or outbound.

For PVCs

`Permanent VC number`

The PVC Number identifies a permanent virtual circuit (PVC) on the remote node. If you have entered a name in the X.25 Address Key field and are configuring PVCs, then you also have to enter a value for the PVC Number.

Configure Neighbor Gateways

Use the next two screens only if you are configuring a node that is on an an X.25 network as a gateway. In this case, the local node needs to know the identity of any **neighbor gateways**.

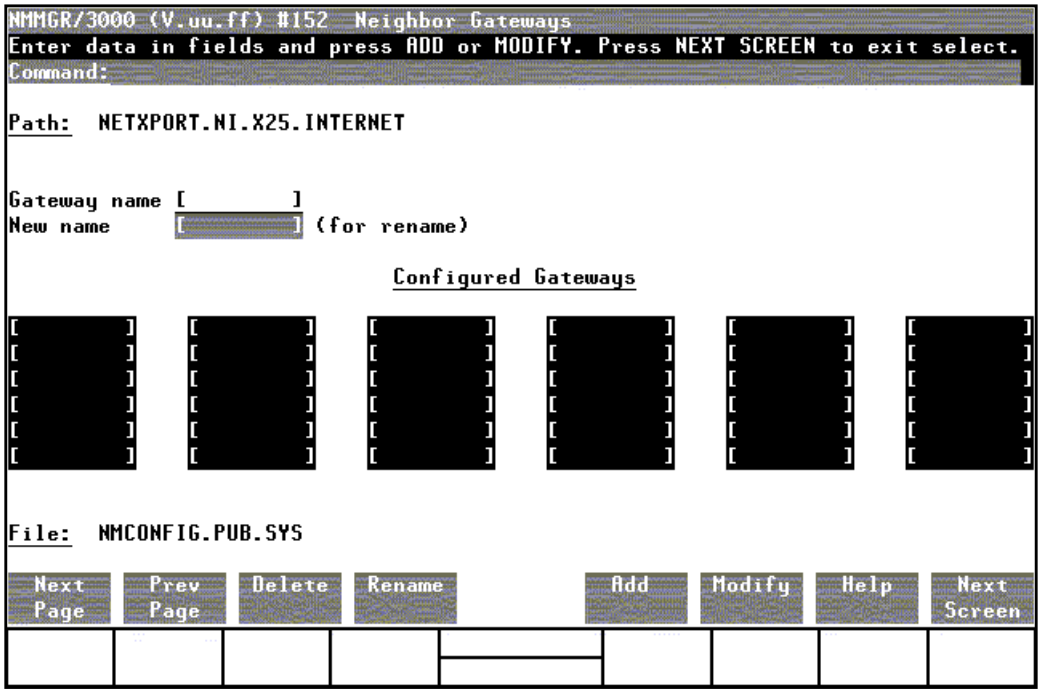
Gateways that are on the same network are called **neighbor gateways**. A non-gateway node on an X.25 network may need to go through a neighbor gateway in order to send messages to an entirely different network. (Two nodes are on the same network if the **network** portion of their IP addresses are the same.) If a node on the X.25 network is trying to access a node on a remote network, it needs to know the identity of its neighbor gateways. When you configure an X.25 node, you enter into its configuration the identity of any accessible neighbor gateways that share the same network. The identified gateways may be either full or half gateways.

You may designate gateways as **default gateways**. Messages for a network will be routed to a default gateway if there is no specific gateway configured for the destination network. The default gateway will then attempt to locate the destination of the message.

Identify Neighbor Gateways (If Any Are Present)

The Neighbor Gateways screen (#152) in Figure 8-4 is displayed when you press the **[Neighbor Gateways]** key at the X.25 Configuration screen (#48) in Figure 8-2.

Figure 8-4 Neighbor Gateways Screen



Step 1. In the `Gateway name` field, enter the name of a gateway that is on the same network as the node that you are configuring. (Nodes are on the same network if the network portions of their IP addresses are the same.).

Step 2. If you are adding the identified gateway for the first time, press the **[Add]** key. If you are modifying the configuration of this node, press the **[Modify]** key. The Neighbor Gateway Reachable Networks screen will be displayed. Proceed to the section titled "To Identify Neighbor Gateway Reachable Networks."

Step 3. Repeat steps 1 and 2 for each gateway that is on the same network as the node that you are configuring. When you have finished, press the **[Prior Screen]** key to return to the X.25 Configuration screen.

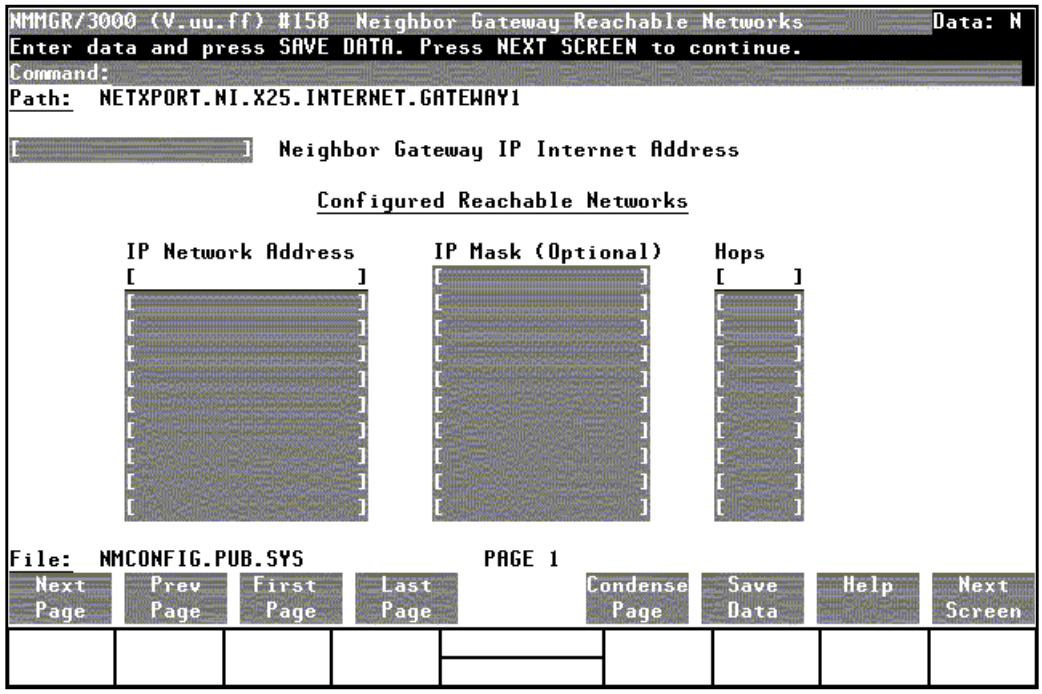
Fields

`Gateway name` Each gateway name can be as long as eight alphanumeric characters. The first character must be alphabetic.

Identify Neighbor Gateway Reachable Networks

The Neighbor Gateway Reachable Networks screen (#158) in Figure 8-5 is displayed when you press the **[Add]** key or the **[Modify]** key for a valid gateway name from the Neighbor Gateways screen (#152) in Figure 8-4.

Figure 8-5 Neighbor Gateway Reachable Networks Screen



Step 1. In the `Neighbor Gateway IP Internet Address` field, enter the IP address of the gateway specified on the Neighbor Gateways screen. An example is: `C 192.007.007 001`

Step 2. In the `IP Network Address` fields under the title `Configured Reachable Networks`, enter the IP addresses of all the remote networks that can be reached through the gateway whose IP address is configured in the previous field.

An "@" in the IP network address field designates the gateway as a default gateway. It means this gateway can be used to reach all the other remote networks.

Step 3. The IP subnet mask is optional. If entering one, tab to the next field. In the `IP mask` field, enter the number in the same format as an IP address.

Step 4. In the field labeled `Hops`, enter the number of hops (full gateways) needed to get to the target network. Two partner gateway halves count as one hop.

Step 5. Repeat steps 2, 3, and 4 for each remote reachable network. The information configured in this screen can extend to more than one page,

if necessary, to allow configuration of up to 2550 reachable networks per link (255 pages and 10 reachable nets per page). If you need to configure more than 10 networks, press the **[Save Data]** key then press the **[Next Page]** key to enter more networks.

Step 6. After you have finished entering the IP addresses of all the reachable networks, press the **[Save Data]** key. Press the **[Prior Screen]** key to return to the Neighbor Gateways screen.

Step 7. Back at the Neighbor Gateways screen, after you have finished adding all of the neighboring gateways, press the **[Prior Screen]** key to return to the X.25 Configuration screen. Follow the instructions for step 7 in the section in this chapter titled "To Configure an X.25 Network."

Fields

If you have identified any neighbor gateways, then you will also be identifying: 1) the IP Network Addresses of all of the networks that you can reach through that gateway, and 2) the number of hops (corresponding to the number of gateways) that a packet passes through to reach a remote network from the local network. Two gateway halves count as one hop.

`Neighbor Gateway IP Internet Address`

The IP address of the gateway whose name you have specified on the Neighbor Gateways Screen. The IP address is in the same format as the LAN Configuration screen.

`IP Network Address`

In the fields under this heading, you list the IP addresses of all of the networks that you will be able to reach through the gateway you are configuring. You also use this field to indicate whether or not the gateway is to serve as a default gateway by entering an at sign (@) to specify that it is a default gateway. Multiple gateways can be designated for each HP e3000 systems.

`IP Mask (Optional)`

The fields under this heading allow you to specify a subnet mask for each reachable network. This mask is optional. For details on deriving an IP subnet mask, see Chapter 2 , "Networking Concepts."

`Hops`

In the fields under this heading, enter the number of hops corresponding to the number of gateways that a packet travels to reach a remote network from a local network.

9 Configuring a Gateway Half

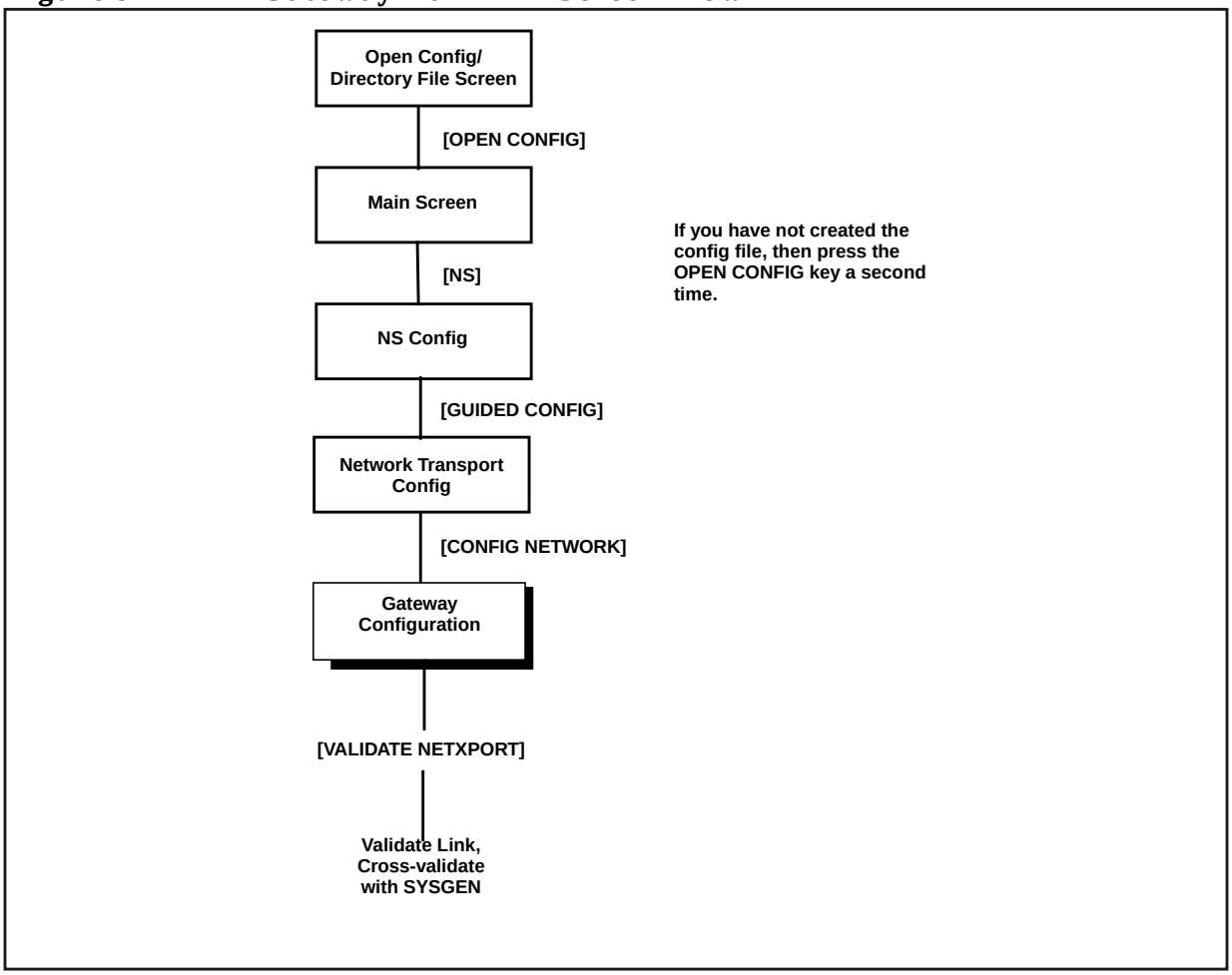
This chapter describes how to plan and configure the interface between one gateway half and another gateway half. Gateway halves is one of the early technologies used to connect two separate networks. For information on configuring a node as a gateway half, use this manual. Gateways are rarely used since the introduction of routers and the internet.

Configuring a node as a gateway half requires configuring two separate network interfaces: one for the serial interface to the remote side of the gateway half, and a second for the gateway half's interface to its home network (for example, a LAN or point-to-point network).

Before configuring a gatehalf, you should have already configured its home network interface, according to instructions in other chapters of this manual.

Figure 9-1 shows the screen flow for configuring gateway half screens. Screens unique to gateway half configuration are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 9-1 Gateway Half Link Screen Flow



Configuring a node as a gateway half requires configuring two separate network interfaces: one for the interface between the two gateway halves, and a second for the gateway half's interface to its home network.

If this gateway half interfaces to a LAN, Token Ring, FDDI, 100VG-AnyLAN, or 100Base-T network, you should have already configured its network interface according to the instructions in Chapter 6 , "Configuring a LAN Node." If this gateway half interfaces to a Point-to-Point or X.25 network, you should already have configured its NI according to instructions in Chapter 7 , "Configuring a Point-to-Point Node," and Chapter 8 , "Configuring a X.25 Node," respectively. If you have not, do so now and then return to this chapter.

This chapter includes step-by-step instructions to help you perform the following tasks:

- Begin the configuration process.
- Configure a gatehalf.

Once the above tasks are completed, refer to Chapter 10 , "Validating

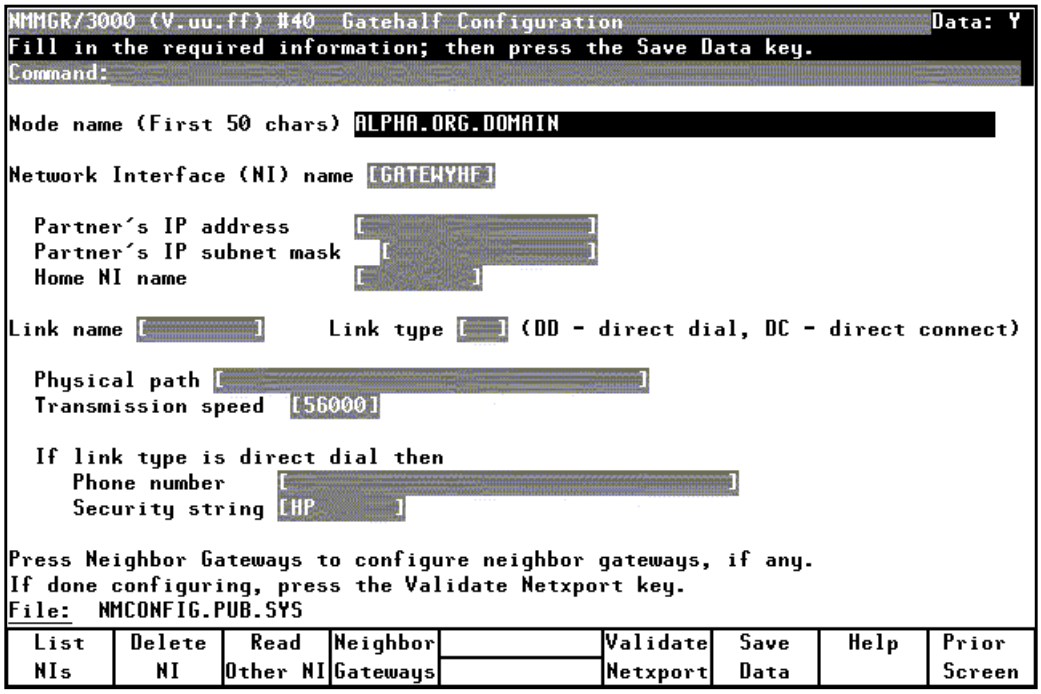
and Cross-Validating with SYSGEN," for step-by-step instructions to help you perform the following validation tasks:

- Validate the network transport configuration.
- Cross-validate in SYSGEN.

Configure a Gatehalf Network Interface

The Gatehalf Configuration screen (#40) in Figure 9-2 is displayed when you press the **[Config Network]** key at the Network Transport Configuration screen (#42) with an NI type of 5 (Gateway Half). Refer to Chapter 5 , “Introductory Screens,” for information on the Network Transport Configuration screen.

Figure 9-2 Gatehalf Configuration Screen



Step 1. In the `Partner's IP address` field, enter the internet protocol (IP) address of this gateway half's partner.

Step 2. The IP subnet mask is optional. If entering one, tab down to the next field. In the IP subnet mask field, enter the number in the same format as an IP address.

Step 3. Tab to the `Home NI name` field. Enter a name that is the same as one of the other network interface names of the node being configured (except gatehalf or loopback networks).

Step 4. Tab down to the `Link name` field and enter a link name to represent each individual hardware interface card.

Step 5. Tab over to the `Link type` field. Enter `DD` for direct dial or `DC` for leased lines, private lines, or other non-switched links.

Step 6. Enter the physical path of this node's Programmable Serial Interface (PSI) card.

Step 7. Tab down to the next field. In the `Transmission speed` field, either leave the default or enter the transmission speed in bits per second as a number from 1200 to 64000.

Step 8. If this is a dial link, enter the phone number of *this* gateway half's *partner*.

Step 9. If this is a dial link, in the `Security string` field, either leave the default, or enter a value that HP nodes must use to gain dial link access to the node you are configuring.

Step 10. Press the **[Save Data]** key. Proceed to Appendix 10 , "Validating and Cross-Validating with SYSGEN," and press the **[Validate Netxport]** key.

`Optional Keys`

Press the **[List NIs]** key to list the names and types of already configured network interfaces.

Press the **[Delete NI]** to remove a configured network interface from the configuration file.

Press the **[Read Other NI]** key to call up a previously configured Network Interface name.

Fields

`Partner's IP address`

This is the internet protocol (IP) address of the node that will be the other half of the gateway half you are configuring. Enter the address in the same format as on the Point-to-Point Configuration screen.

`Partner's IP subnet mask`

Allows you to specify the subnet mask of this gateway half's partner gateway half. The 32-bit mask is grouped in octets expressed as decimal integers and delimited by either a period (.) or a space. The mask identifies which bits of an IP address will be used to define a subnetwork. To determine these bits, you first need to estimate how many subnetworks and nodes per subnetwork you need. For details on deriving an IP subnet mask, see Chapter 2 , "Networking Concepts."

`Home NI name`

The home NI name will be used by the software to determine which network address is the source network address when packets are sent over the gateway half. The home NI name cannot be either a gateway half or loopback NI name, but it can refer to any other type of network interface (LAN, Token Ring, Point-to-Point, FDDI, or X.25 network interface).

`Link name`

Name that represents the hardware link. The link name can have up to eight alphanumeric characters; the first character must be alphabetic. The link name must be unique to both the node and the network.

`Link type`

The link type for a gateway half can be either `DD` for direct dial or `DC` for direct connect.

`physical path`

The physical path number corresponds to the slot location of a node's programmable serial interface (PSI) card or, Advanced Communication Controller (ACC) for N 4000 and A500 systems. Recommended slot locations and physical path calculations vary according to the type of HP e3000 system you are running.

For the various platforms, physical path syntax (examples only) look like:

Series 9x7:	48	PSI
Series 9x8:	56/44	PSI
Series 9x9:	10/4/16	PSI
Series 99x:	0/28/12	PSI
Series N 4000:	1/10/0/1.7	ACC
Series A500:	0/2/0/1.4	ACC

If you are unsure of the slot location or of the physical path number to configure for your system, run the offline ODE MAPPER utility, see your system documentation, or consult your Hewlett-Packard service representative.

`Transmission speed`

The line transmission speed is given in bits per second. For direct connect the value, must be supported by both adapter and cable. Values are 1200, 2400, 4800, 9600, 19200, 38400, 56000, and 64000. The default is 56000.

`Phone Number`

Telephone number of this gateway half's partner gateway half. Enter the telephone number as a combination of decimal numbers (`0` through `9`), dashes, and the following special characters:

`/`	Separator used for automatic call units that have second dial-tone detect.
`E`	Optional end-of-number indicator.
`D`	Three-second delay (used for European modems and automatic call units that require built-in delays).
#	Defined by local phone system.
*	Defined by local phone system.

Spaces, and left and right parentheses ( ) are also allowed.

To disable outbound dialing, enter an exclamation point (`!`) by itself in the phone number field.

`Security string`

This is a string containing up to eight alphanumeric characters, left justified, with no embedded blanks. The first character must be alphabetic. A value in this field is required if the remote (destination) node is an HP node (dial ID protocol is used). Remote HP nodes must use the security string to gain dial link access to the node you are configuring.

10 Validating and Cross-Validating with SYSGEN

This chapter discusses the validation of the network transport configuration and cross-validation of NMCONFIG.PUB.SYS with the system configuration files within SYSGEN.

Validating the network transport. This step checks data consistency between values entered on different NMMGR data entry screens. Cross-Validating with SYSGEN.

Cross-validation ensures that there are no conflicts in the use of node names, device classes, and physical paths.

Validate the Network Transport

The following procedure assumes that you have already configured and validated the Distributed Terminal Subsystem (DTS). The DTS must be validated before you can validate the network transport (Netxport) software. Upon configuring the selected screens for your network:

Step 1. Press the **[Validate Netxport]** key. Refer to the list of screens with the **[Validate Netxport]** key.

LAN, 100Base-T, or 100VG-AnyLAN — Figure 6-2
Token Ring — Figure 6-3
FDDI — Figure 6-4
Point-to-Point Shared Dial — Figure 7-5
Point-to-Point Direct Dial — Figure 7-6
X.25 — Figure 8-3
Gateway Half — Figure 9-2
Logging — Figure 13-2

Messages similar to the following ones will be displayed:

```
Searching for subsystem validation routine VALIDATEDTS
---> Validation of DTS/LINK started. <---
---> Validation of DTS/LINK finished. <---
NMMGR will now cross-validate the NMCONFIG file with SYSGEN.

SYSGEN version V.uu.ff : catalog version V.uu.ff    WED, NOV 15, 2000, 11:10 AM
Copyright 1987 Hewlett-Packard Co. All Rights Reserved.

        **note** Retrieving NMMGR configuration data...

** First level command **

        io              log (lo)       misc (mi)        spu (sp)
        sysfile (sy)

        basegroup (ba)  keep(ke)       permyes (pe)     show (sh)
        tape (ta)

        clear (cl)(c)   exit (ex)(e)   help (he)(h)     oclose (oc)
        redo
sysgen> PERMYES ON
sysgen> BA CONFIG
sysgen> SY
```

```
        ** SYSFILE configurator commands **

        aauto (aa)      aboot (ab)     acmsl (ac)        asprog (as)
        cmsl (cm)       dauto (da)     dboot (db)        dcmsl (dc)
        dsprog (ds)     lcmsl (lc)     rauto (ra)        rboot (rb)
        rcat (rc)       rcmsl (rcm)    rdcc (rd)         ripl (ri)
        rnmlib (rn)     rsprog (rs)    show (sh)

        clear (cl)(c)   exit (ex)(e)   help (he)(h)      hold (ho)
sysfile> RDCC

        **note** Retrieving NMMGR configuration data...
sysfile> HO

sysfile> EX

 sysgen> KE

        keeping to group CONFIG.SYS
        Purge old configuration (yes/no)?Automatic yes
        ** configuration files successfully saved **
 sysgen> EX


Cross-validation with SYSGEN was successful.

Copying validated configuration file to backup file, please wait ***

(Press RETURN when done viewing screen contents)
```

Step 2. See the *NS 3000/iX Error Messages Reference Manual* for explanations of any validation errors. After viewing the messages, press **[RETURN]** to return to the LAN, Token Ring, FDDI, 100VG-AnyLAN, and 100Base-T Configuration screen.

Step 3. If you need to configure a network directory, proceed to Chapter 11 , “Configuring the Network Directory.” If you do not need to configure the network directory, exit NMMGR, and proceed to the section in this chapter titled “To Cross-Validate in SYSGEN.” To exit NMMGR, press the **[Prior Screen]** key on successive screens until you reach the Open Configuration Directory File screen where you should press the **[Exit Program]** key.

Cross-Validate in SYSGEN

Cross-validation is automatically done on the KEEP, TAPE, I/O, and RDCC commands in SYSGEN.

Cross-validation ensures that there are no conflicts in the use of node names, device classes, and physical paths between the data currently contained in NMCONFIG.PUB.SYS and the system configuration data.

To cross-validate, use the SYSGEN facility (OP capability is required). To use SYSGEN, type the following commands at the MPE prompt:

```
:sysgen        sysgen> io
               io> ld (optional)
               io> exit
               sysgen> exit
```

The optional ld (list devices) command allows you to verify the NMMGR devices that are configured. For more information, see System Startup, Configuration, and Shutdown.

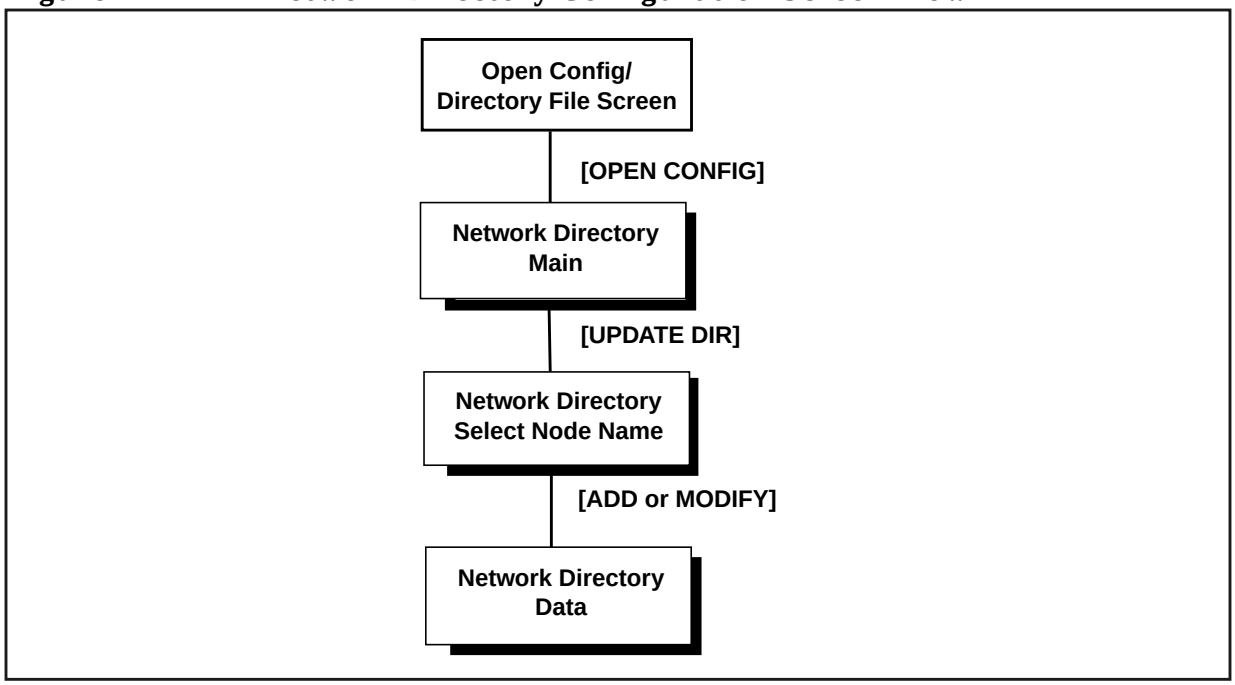
If you have completed the configuration process, proceed to Chapter 14 , “Operating the Network.”

11 Configuring the Network Directory

A network directory is used by the node for internetwork routing. It is one of several ways of specifying fixed/hardcoded addresses for specific node names, in cases where dynamic name resolution cannot be used. It is also used for specifying unique node names for a system which has multiple interfaces. Each entry in a network directory consists of a node name associated with an IP address, the network type, and an additional address, if necessary. The network directory uses the internet protocol (IP) address to transfer data between networks. See Chapter 2 , “Networking Concepts,” for more information on network directory concepts and for guidelines as to when you need to configure a network directory.

Figure 11-1 shows the screen flow for configuring the network directory screens. Screens unique to the network directory configuration are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 11-1 Network Directory Configuration Screen Flow



This chapter includes step-by-step instructions to help you perform the following tasks:

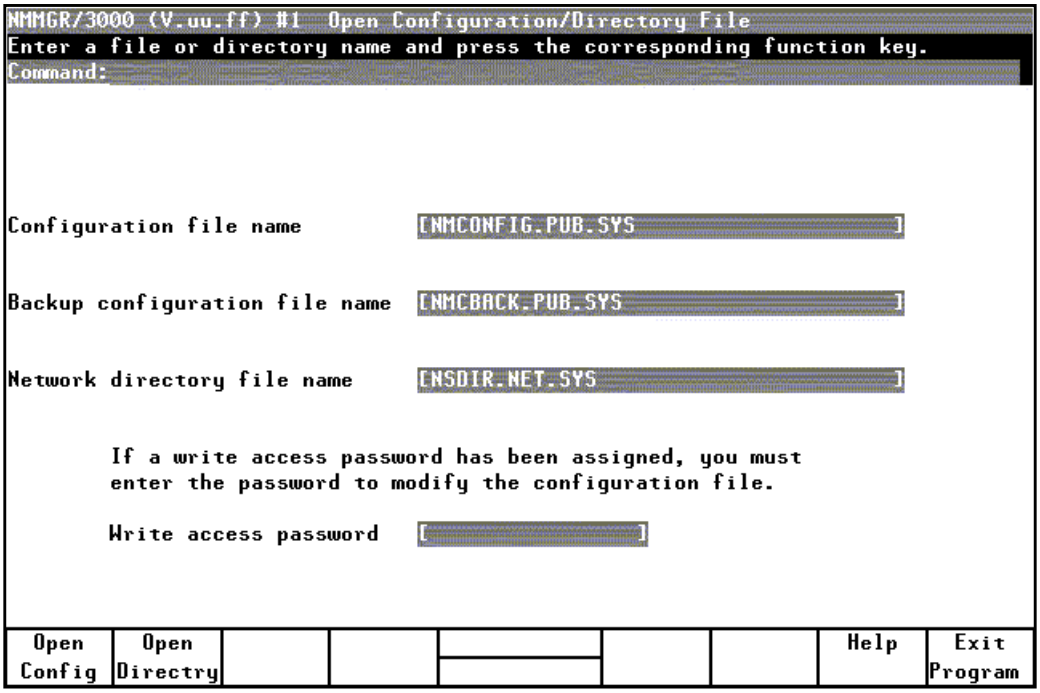
- Open the network directory file.
- Select the update directory function.
- Add nodes to the network directory file.
- Configure path report data for a node.

NOTE If you used the guided configuration facility to configure an X.25 link, you will already have configured the network directory for that link.

Open Network Directory

The Open Configuration/Directory file screen (#1) in Figure 11-2 is the first screen displayed when you run NMMGR.

Figure 11-2 Open Configuration/Directory File



Step 1. Verify that the correct network directory file name is in the `Network directory file name` field.

Step 2. If you have assigned a write access password, enter it in this field. If you are not using the password feature, leave this field blank.

Step 3. Press the **[Open Directry]** key. If you are creating the file for the first time, NMMGR will ask you to verify creation. Press the **[Open Directry]** key again to continue.

Fields

`Configuration file name`

The only configuration file name the system recognizes for use by the network subsystem is `NMCONFIG.PUB.SYS`. You can, however, create or modify a configuration file using a different name and save it as an **offline configuration file**. You can use offline configuration files as a means of creating and storing configurations that you want to use in the future or that you are preparing for use on a different system.

When you are ready to use an offline configuration file, rename it as NMCONFIG.PUB.SYS and reboot the system. (Keep in mind that any file you use as a configuration file must be successfully validated before you try to use it.)

`Backup configurationfile name`

A backup file name must be specified whenever a configuration file is opened or created. The default backup configuration file name is NMCBACK.group.account. The backup file will be automatically updated with the contents of the configuration file each time the configuration file is successfully validated.

`Network directory file name`

The only network directory file name supported by HP is NSDIR.NET.SYS. This file is part of a KSAM pair. A key file is created at the same time as this data file. The key file will automatically be named using the first six letters of the network directory file name, appended with the character K. For example, NSDIRK.NET.SYS is the name of the key file associated with the data file NSDIR.NET.SYS. If the name of the data file is less than six letters long, then the entire file name would be appended with a K.

`Write access password`

The password is an optional feature. If a password has been assigned, you must enter it in the password field to update the configuration file or the directory file. It is still possible to open an existing file without using an assigned password, but the file will be in read only mode and no changes will be accepted.

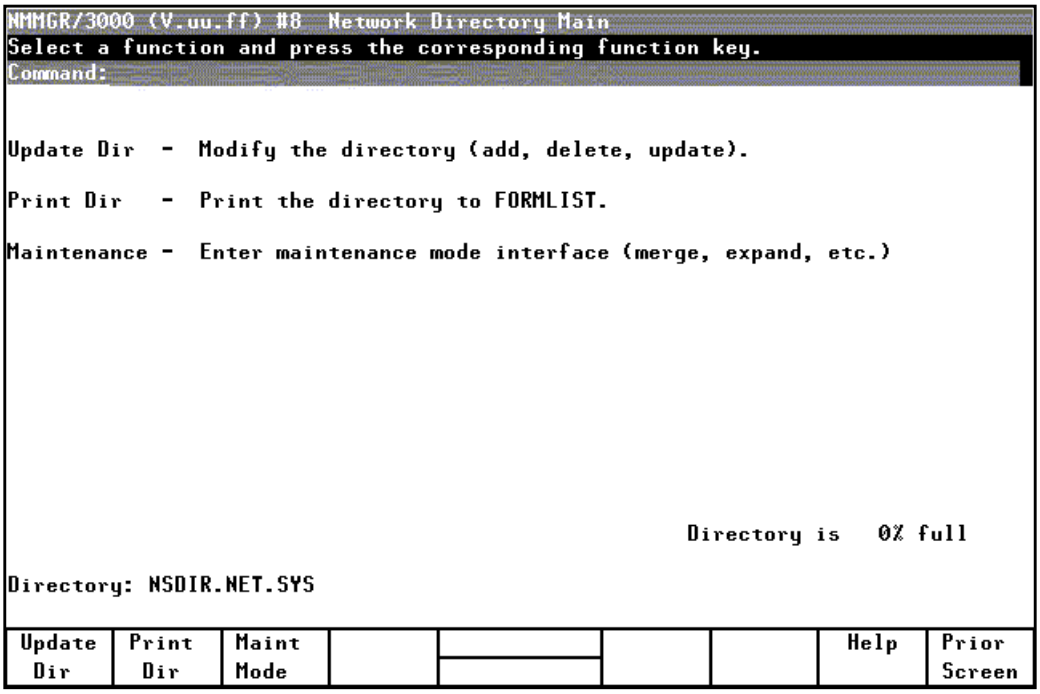
If a password has not been assigned, you should ignore the password field.

If you want to assign a password for the system you are configuring, see *Using the Node Management Services (NMS) Utilities*.

Select Update Directory Function

The Network Directory Main screen (#8) in Figure 11-3 is displayed when you press the **[Open Directry]** function key at the Open Configuration/Directory File screen (#1) in Figure 11-2. This screen is also displayed if a network directory has already been opened and you type NETDIR in the command window of any screen and press the **[Enter]** key.

Figure 11-3 Network Directory Main



Step 1. Press the **[Update Dir]** function key to modify the contents of the directory by adding, deleting and updating node names and path reports.

Function Keys

This screen is the main select screen from which all directory functions are accessed. The currently opened directory is displayed at the bottom of all network directory screens. The percentage of the network directory that is full is shown in the lower right corner of the screen.

`Update Dir` Press this function key to go to the Network Directory Select Node Name screen to add, delete, or modify network directory node name entries and path reports.

`Print Dir` Press this function key to print out a copy of the directory to formal designator FORMLIST, device class LP. You can use a file equation for FORMLIST to redirect

the output to another device class or disk file. To set a file equation without leaving NMMGR, enter the appropriate MPE command in the command window and press the **[Enter]** key.

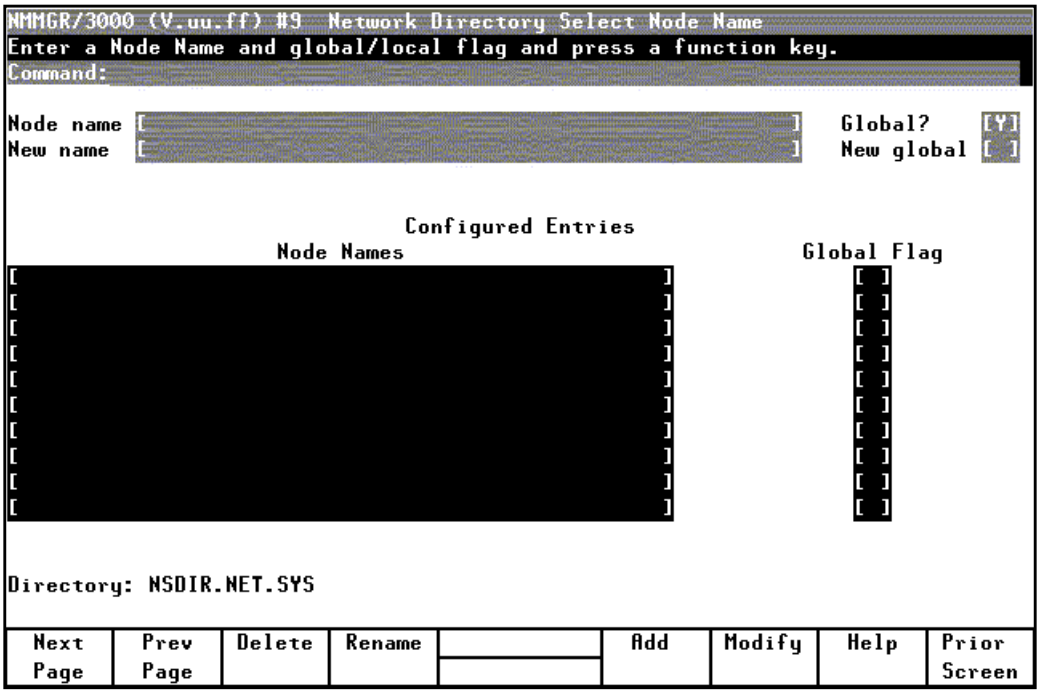
`Maint Mode` Press this function key to enter the command interface to perform directory merging or to expand the size of your directory. See *Using the Node Management Services (NMS) Utilities* for details on maintenance mode.

Within the maintenance mode interface, command input is read from the formal designator `NMMGRCMD`, which defaults to `$STDINX`. Type `EXIT` and press the **[Return]** key to leave maintenance mode.

Add Nodes to Network Directory File

The Network Directory Select Node Name screen (#9) in Figure 11-4 is displayed when you press the **[Update Dir]** function key at the Network Directory Main screen (#8) in Figure 11-3. The function of this screen is to display node names that are currently configured in the directory, and to allow you to delete, rename, add, or modify information about a node.

Figure 11-4 Network Directory Select Node Name



Step 1. In the node name field, type in the node name of one of the nodes on your network for which you want network directory information.

Step 2. Set the global/local flag for the entry by setting the value in the Global? field. Leave the default (Y) if you want to allow this entry to be merged into other directories using the MERGEDIR command. Change the setting to "no" (N) if this is a local entry and should not be copied to other configurations.

Step 3. Press the **[Add]** function key. You may add new entries as long as room remains in the file. If the file fills, you may use the Maintenance Mode command EXPANDDIR to expand the file. Refer to *Using the Node Management Services (NMS) Utilities* for details on maintenance mode.

Step 4. Repeat steps 1, 2, and 3 for each node name you want to enter in the network directory.

Fields

`Node name`

The name of the node for which you want network directory information. The node name field must contain a fully qualified node name, in the form `nodename.domain.organization`, when used to add, modify, delete, or rename a node.

The node name field when used with the `Prev Page` and `Next Page` function keys allows you to browse through a specified part of the network directory. You can enter part of a node name in this field to designate which node names you want displayed. For example, if you enter the value `NIK`, and press the **[Next Page]** function key, the list of nodes will begin with the first matching node name, for example `NIKOLAI.FINANCE.IND`, and continue through the rest of the alphabet until all node names between the letters `NIK` and `Z` are listed.

`Global?`

The global/local setting for node name. The acceptable values are `Y` or `N`. When the `Prev Page` and `Next Page` function keys are used, only node names whose global/local setting matches the value in this field are displayed.

Entries can be configured as either global or local in the network directory. **Global** entries (the default) can be merged into other directories using the `MERGEDIR` command. Local entries are not merged into other network directories. The local entries are used for configuring localized network directory entries, thus providing a mechanism to restrict directory data from being propagated throughout the network.

A situation where this type of restriction could be useful is when you want to change the configuration for users on a single host, but not for everyone else. You can configure two network directory entries: one local, used by host users, and one global, used by everyone else when establishing connections to the host. For example, suppose Node A sets up a new link to Node C, but Node A does not want other nodes (already connected to A) to know about Node C until the new link is tested. Users on Node A can configure a local entry, which contains information about the new link not included in the global entry configured for users on other nodes.

Other uses of local entries include restricting certain nodes from communicating with the internet, or being able to direct which way to access remote nodes depending on your configuration of local entries. When

both local and global entries exist for the same node, the network transport uses the local entry.

Default value: Y

Range: Y or N

`New name` (Required only when renaming an existing node name.) New name to be assigned to the node with the `Rename` function key.

`New global` The global/local flag setting for the node named in the new name field. The acceptable values are Y or N. The only time this field is used is when you rename a node or when you change the global/local setting of a node. The new name field can be left blank if you wish to change only the global/local setting.

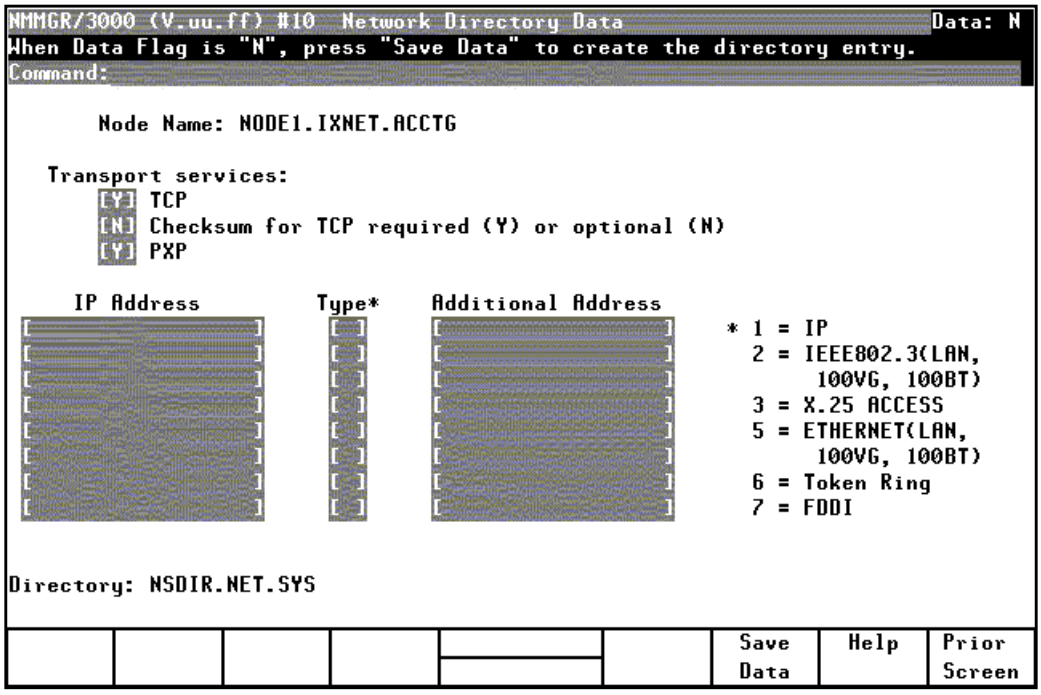
`Configured Entries (node names & global flag)`

Display-only fields that show node names and their global/local flag settings that are already configured in the directory.

Configure Path Report Data for a Node

The Network Directory Data screen (#10) in Figure 11-5 is displayed when you press the **[Add]** or the **[Modify]** function key at the Select Node Name screen (#9) in Figure 11-4.

Figure 11-5 Network Directory Data



The function of this screen is to configure path report data for the node name listed at the top of the screen. One path report is configured for each NI on a node. Because the maximum number of NIs per node is 48 (including loopback), each node can contain as many as 47 path reports.

Step 1. Verify that the yes and no indicators in the TCP, Checksum for TCP required, and PXP fields are set correctly.

Step 2. In the IP address field, type in the IP address of the node listed in the Node name field.

Step 3. In the type field, enter the number that indicates the type of the path:

1 = IP
2 = LAN/IEEE 802.3 (LAN, 100VG, 100BT)
3 = X.25 ACCESS
5 = ETHERNET (LAN 100VG, 100BT)
6 = Token Ring, 100VG/IEEE 802.5
7 = FDDI

Step 4. If appropriate for the type of path you are configuring, enter an address in the Additional Address field. (Type 1 requires no additional address. Types 2, 5, and 6 require a station address. Type 3 requires an X.25 address key. See additional explanation under "Fields."

Step 5. Press the **[Save Data]** key.

Step 6. Repeat steps 2, 3, and 4 for each path report for the specified node.

If you need to make additional entries in the network directory, press the **[Prior Screen]** key to return to the Network Directory Select Node Name screen. If you have finished making network directory entries, home the cursor and type EXIT in the command field, then press **[ENTER]**.

Fields

Transport services

These three fields describe the transport services that should be configured in each path.

TCP	TCP must be Y (yes) for all nodes. The default is Y.
Checksum for TCP	The checksum setting indicates whether checksumming is optional (N) or required (Y) for TCP. If this field is set to N, then the use of checksums is not requested when communicating with this node. If this field is set to Y then checksums are used when communicating with this node. Checksumming is required for communication to non-HP systems. The default is N.
PXP	PXP must be Y (yes) for all nodes. The default is Y.

Note that the selection of transport services here must match the settings in the remote node's configuration file. If the checksum enabled field in the path NETXPORT.GPROT.TCP of this node is set to Y, then TCP checksum field in the network directory should also be set to Y.

IP address	One IP address should be entered for each network interface configured on the remote node that is directly reachable from this node. Each address must match an IP address configured in the remote node's configuration file. The path of the screen in the configuration file that contains IP addresses is NETXPORT.NI.*NIname*.PROTOCOL.IP.

Type — A number indicating the type of path to configure:

- 1 — Select this path type when the NI type is ROUTER (Point-to-Point); or when the NI type is LAN and the destination node supports probe or ARP; or when the NI type is TOKEN or FDDI and the destination node supports ARP.
- 2 — Select this path type when the NI type is LAN, 100VG-AnyLAN or 100Base-T, the destination node does not support probe, and 802.3 framing is used.
- 3 — Select this path type when the NI type is X25.
- 5 — Select this path type when the NI type is LAN, 100VG-AnyLAN or 100Base-T, the destination node does not support ARP or probe, and Ethernet framing is to be used.
- 6 — Select this path type when the NI type is TOKEN and the destination node does not support ARP.
- 7 — Select this path type when the NI type is FDDI and the destination node does not support ARP.

Table 11-1 Path Type Configuration

N1 Type	Framing	Protocols	Type
Point-to-Point (Router)	N/A	N/A	1
LAN	802.3 and Ethernet	Either Probe or ARP	1
	802.3 and Ethernet	Neither Probe nor ARP	5
	802.3 only	Not Probe	2
	Ethernet only	Not ARP	5
X.25	N/A	N/A	3
Token Ring	N/A	ARP	1
	N/A	Not ARP	6
FDDI	N/A	ARP	1
	N/A	Not ARP	7

`Additional address`

A lower-level address, which depends on the type.

Type `1` does not contain lower-level addressing information. You can leave the field blank, or enter the keyword `NONE`.

Types `2`, `5`, `6`, and `7` require the destination node's station address, which is a string of six hexadecimal bytes, separated by dashes (`XX-XX-XX-XX-XX-XX`). The station address must correspond to the address configured on the remote node.

Type `3` requires an X.25 address key, which is an ASCII string of up to 15 characters. The X.25 address key must correspond to an X.25 address key entered in the `NETXPORT.NI.`*`NIname`*`.PROTOCOL.X25.SVPATH` or the `NETXPORT.NI.`*`NIname`*`.PROTOCOL.X25.PVCPATH` screen for the destination node.

12 Configuring Domain Name Files

If you are planning to use the domain name resolver for name to IP address resolution, you will need to configure a set of ASCII files on each node that contain needed information. To configure these files, you use any standard editor to modify existing sample files according to the instructions in this chapter. See Chapter 2 , “Networking Concepts,” for more information on domain names.

This chapter details:

- How to modify the `RSLVSAMP.NET.SYS` file and save it as `RESLVCNF.NET.SYS` for use as the domain name resolver.
- How to modify the `HOSTSAMP.NET.SYS` file and save it as `HOSTS.NET.SYS` for use as the domain name host file.
- Other files you can configure to make additional information available to the network.

Create or Modify the Resolver File

The resolver file (RESLVCNF.NET.SYS) is an initialization file for the domain name resolver. It contains information needed by the network to determine how to resolve a domain name to an IP address. This file is read by the resolver routines the first time they are invoked by a process.

To create the resolver file, perform the following steps:

Step 1. Copy the sample file, RSLVSAMP.NET.SYS, to RESLVCNF.NET.SYS.

Step 2. Modify RESLVCNF.NET.SYS using any ASCII editor so that it contains information about the name servers, domain, and search order for your network. The keywords included in the file are described under "Fields."

To modify an already existing RESLVCNF.NET.SYS file, simply use your editor to update and save the existing file.

Fields

Each entry in the resolver file consists of a keyword followed by a value separated by white space. The keyword and its associated value must appear on a single line and the keyword must start the line. Figure 12-1 shows an example of a resolver file. Comment lines start with a pound sign (#).

`domain` Enter the local domain name. Most queries for names within this domain can use short names relative to the local domain name. If the host name does not contain a domain part, the root domain is assumed. If more than one instance of the `domain` keyword is present, the last instance will override.

The domain name is composed of labels, with each label separated by a period. Each label must start with a letter or digit, and have as interior characters only letters, digits, hyphens (-), or underbars (_). A domain name may have any number of labels, but its total length, including periods, is limited to 255 characters.

```
label[.label][...]
```

Domain names are not case sensitive.

`search` The `search` entry is optional and indicates the order in which domains should be searched for host name lookup. You should add a `search` entry if users on this system commonly try to connect to nodes in other domains. The search list is limited to six domains with a total of 256 characters. If more than one instance of the `search` keyword is present, the last instance will override.

Resolver queries will be attempted using each component of the search path in turn until a match is found. Note that this process may be slow and will generate a lot of network traffic if the servers for the listed domains are not local. Note also that queries will time out if no server is available for one of the domains.

`nameserver` Enter the IP address of a name server the resolver should query. The address must be in dot format, with leading zeros omitted and a period between each grouping. See example addresses in Figure 12-1.

NOTE It is very important that you omit the leading zeros in the network addresses that you enter in the domain name resolver files. If you enter leading zeros here, the domain name resolver will interpret the numbers as octal numbers.

You can list up to three name servers, but you must use a separate keyword entry for each. If there are multiple servers, the resolver will query them in the order listed. If no `nameserver` entries are present, the default is to use the `HOSTS.NET.SYS` file.

If you have no server, do not add any `nameserver` entries; the resolver will immediately revert to the `HOSTS.NET.SYS` file.

Errors in the resolver file will be silently ignored by the resolver routines.

Figure 12-1 Sample Resolver Configuration File

```
#resolv.conf file
#
domain loc1.inet.com
search loc1.inet.com inet.com
nameserver 192.255.25.33
nameserver 192.255.354.74
nameserver 192.15.360.75
```

NOTE The IP addresses and domain names used in Figure 12-1 are for purposes of the example only.

Create or Modify the Hosts File

The host name data base file, (HOSTS.NET.SYS), associates internet addresses with official host names and aliases. This allows a user to refer to a host by a symbolic name instead of an internet address.

When you have configured the name server, this file serves only as a backup when the server is not running. In this circumstance, it is a common practice that HOSTS.NET.SYS contains a few addresses of machines on the local network.

To create the hosts file, perform the following steps:

Step 1. Copy the sample file, HOSTSAMP.NET.SYS, to HOSTS.NET.SYS.

Step 2. Modify HOSTS.NET.SYS using any ASCII editor so that it contains information about the nodes on your network.

To modify an already existing HOSTS.NET.SYS file, simply use your editor to update and save the existing file.

Enter a single line for each host, including the following information:

```
[internet address] [local host name] [aliases]
```

A line cannot start with a space. Items are separated by any number of blanks and/or tab characters. A pound sign (#) indicates the beginning of a comment.

Network addresses are specified in dot format, with leading zeros omitted and a period between each grouping. (See example addresses in Figure 12-2.)

Host names can contain any printable character other than a white space, newline, or comment character.

NOTE It is very important that you omit the leading zeros in the network addresses. If you enter the leading zeros here, the domain name resolver will interpret the numbers as octal numbers.

Figure 12-2 Sample Hosts Configuration File

```
# This file contains information regarding the known hosts.
#
# The for for each entry is:
# host IP address     local host name     host aliases
#
# Note: the entries cannot be preceded by a blank space.
#
172.0.0.1       localhost loopback me myself local
192.41.12.100   basful.loc1.inet.com          bashful
192.41.11.114   happy.loc1.inet.com           happy
192.41.11.413   queezy.loc1.inet.com          queezy
192.41.112.122  sneezy.loc2.inet.com          sneezy
192.41.124.4    mpmndda.loc1.inet.com         mpmndda    moose
192.41.124.6    mpmndwa.loc1.inet.com         mpmndwa    wabbit
192.41.114.132  mpmtchq.loc1.inet.com         mpmtchq    foo
192.41.110.16   mpmndiv.loc1.inet.com         mpmndiv    zephyr
192.41.110.82   abacus.loc1.inet.com          abacus     spots
192.41.112.161  camelot.loc1.inet.com         camelot
192.41.112.166  bigblue.loc1.inet.com         bigblue
```

NOTE The IP addresses and host names used in Figure 12-2 are for purposes of the example only.

Additional Domain Name Configuration Files

In addition to the resolver file and the host name data base, three other files are available to allow you to configure additional information about your network. Each of these files is provided in sample format in the NET.SYS account. Each sample file contains an explanation of the format for the data and a sample entry. The available files and their functions are described as follows.

Network Name Database

The network name database, NETWORKS.NET.SYS, associates IP addresses with official network names and aliases. This allows the user to refer to a network by a symbolic name instead of an internet address. To configure the network name database, modify the sample file NETSAMP.NET.SYS.

Protocol Name Database

The protocol name database PROTOCOL.NET.SYS, associates protocol numbers with official protocol names and aliases. This allows the user to refer to a protocol by a symbolic name instead of a number. The protocol number mappings are defined in *RFC 1010 Assigned Numbers*. To configure the protocol name database, modify the sample file PROTSAMP.NET.SYS (this is required for FTP use, starting in release 6.0).

Service Name Database

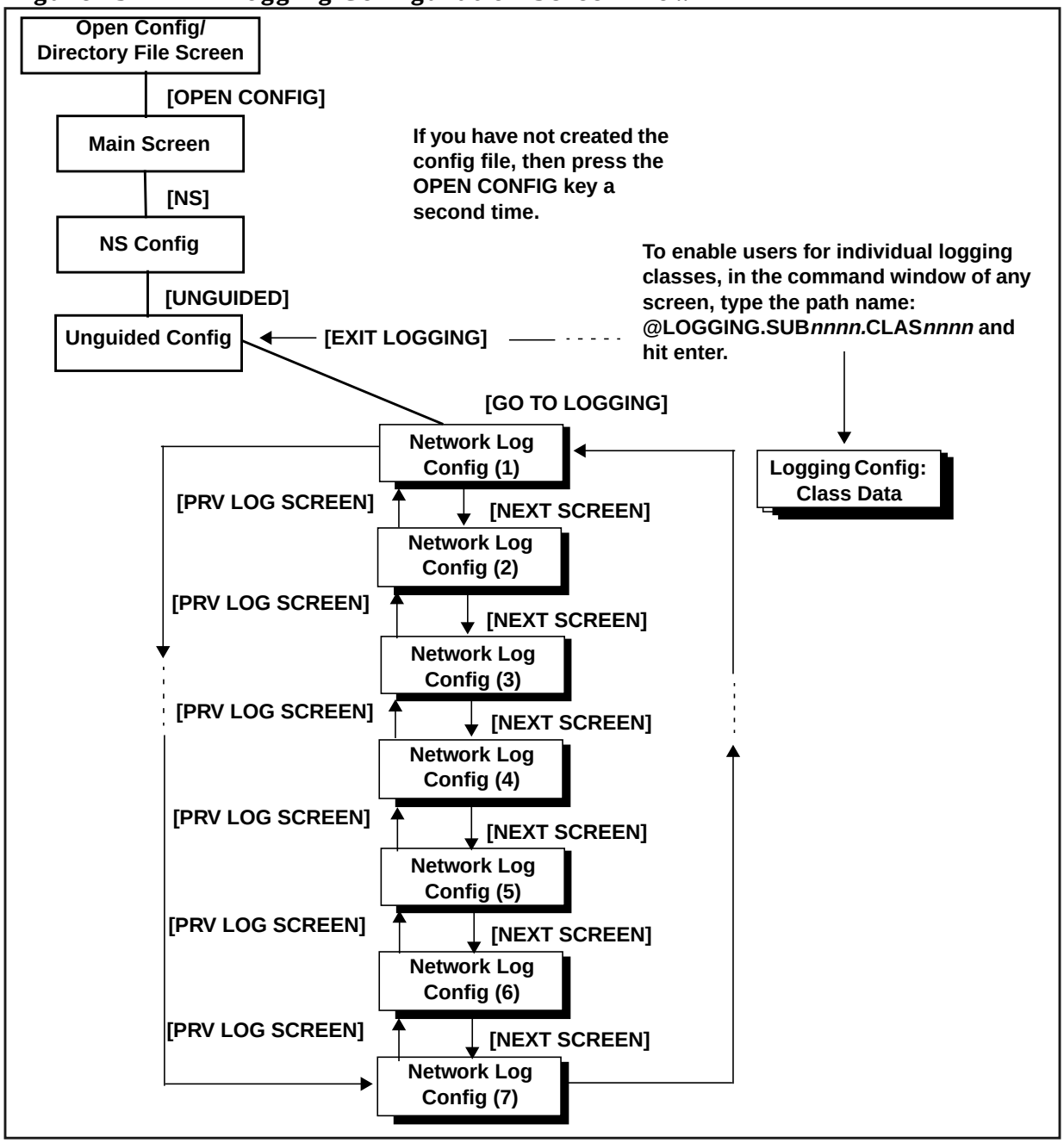
The service name database, SERVICES.NET.SYS, associates official service names and aliases with the port number and protocol the services use. Reserved port numbers 0 through 255 are assigned by RFC 1010. To configure the service name database, modify the sample file SERVSAMP.NET.SYS.

13 Configuring Logging

This chapter provides step-by-step instructions for configuring logging. Logging is configured for the purpose of recording events such as errors and console commands.

Figure 13-1 shows the screen flow for configuring the logging screens. Screens unique to logging are indicated by bold boxed screens. **[FUNCTION]** denotes the function key used at a screen to invoke the next screen on the screen flow.

Figure 13-1 Logging Configuration Screen Flow



This chapter includes step-by-step instructions to help you perform the following tasks:

- Access the logging configuration screens.
- Modify the logging configuration.
- Enable users for individual logging classes.
- Activate logging.

Logging is configured for the purpose of recording events such as errors and console commands. You configure logging for each of the subsystems of NS 3000/iX and for NS 3000/iX links. Each subsystem includes different classes of events (such as internal errors). You can record logging to a disk file for later analysis, to the system console so that the system operator receives the messages, or both.

You can also display logging events at individual users' list devices. This may be valuable to allow the network manager to monitor NS console activity from an alternate terminal. If you configure a logging class so that logging is recorded to a user.account, the user will receive logged messages any time there is an active session for that user.account. (Take care if you enable users for logging; doing so can place a strain on system resources.)

The guided configuration process configures logging for you using defaults. You can also configure or modify the logging subsystem using either guided or unguided configuration.

Access Logging Configuration Screens

Use the following steps to reach the logging configuration screens:

Step 1. Run NMMGR. The Open Configuration/Directory File screen is displayed.

Step 2. Press the **[OPEN CONFIG]** key. The Main screen is dispayed.

Step 3. Press the **[NS]** function key. The NS Configuration screen is displayed.

Step 4. Press either the **[Guided Config]** or the **[Unguided Config]** function key.

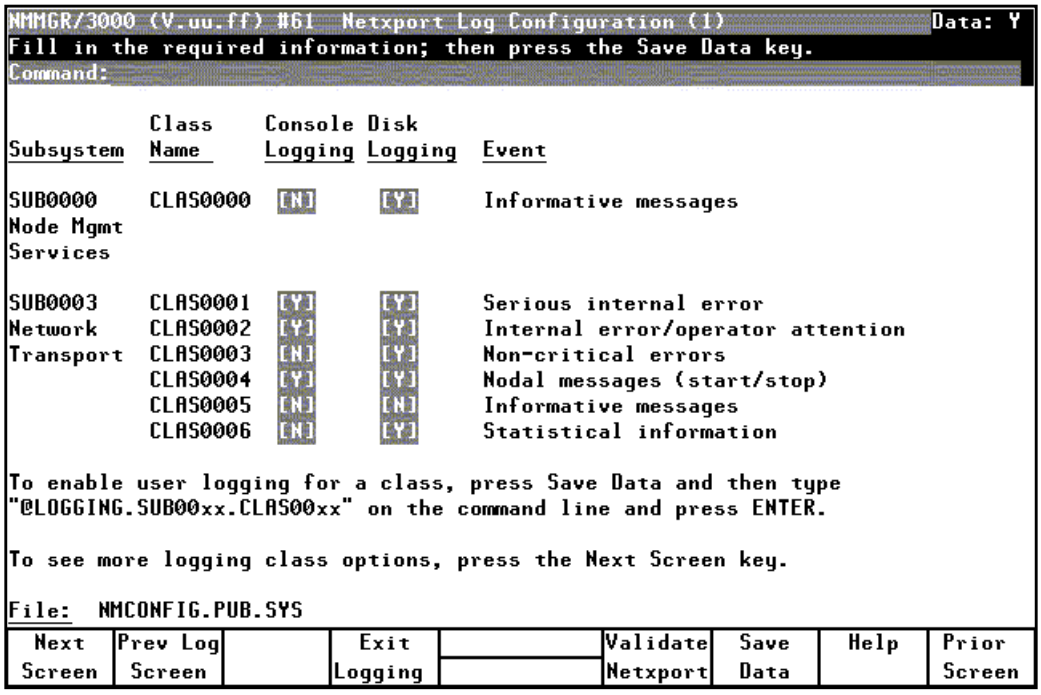
Step 5. Press the **[Modify Logging]** function key if you are in guided configuration or the **[Go To Logging]** function key if you are in unguided configuration. The first of seven logging configuration screens is displayed.

NOTE HP recommends that you use the default logging configuration values unless your HP representative tells you otherwise. Not using the recommended default values may result in the degradation of system performance.

Modify the Logging Configuration

The Netxport Log Configuration (1) screen (#61) in Figure 13-2 is displayed when you press the **[Modify Logging]** function key at the Network Transport Configuration screen.

Figure 13-2 Netxport Log Configuration (1) Screen



```
NMMGR/3000 (V.uu.ff) #61  Netxport Log Configuration (1)          Data: Y
Fill in the required information; then press the Save Data key.
Command:

            Class     Console Disk
Subsystem   Name      Logging Logging  Event

SUB0000     CLAS0000  [N]     [Y]      Informative messages
Node Mgmt
Services

SUB0003     CLAS0001  [Y]     [Y]      Serious internal error
Network     CLAS0002  [Y]     [Y]      Internal error/operator attention
Transport   CLAS0003  [N]     [Y]      Non-critical errors
            CLAS0004  [Y]     [Y]      Nodal messages (start/stop)
            CLAS0005  [N]     [N]      Informative messages
            CLAS0006  [N]     [Y]      Statistical information

To enable user logging for a class, press Save Data and then type
"@LOGGING.SUB00xx.CLAS00xx" on the command line and press ENTER.

To see more logging class options, press the Next Screen key.

File:  NMCONFIG.PUB.SYS
```

Next Screen	Prev Log Screen		Exit Logging		Validate Netxport	Save Data	Help	Prior Screen

Use the fields and the function keys of the screen to configure logging for the subsystems represented on the screen. If the subsystem for which you want to enable logging does not appear on the first screen, press the **[Next Screen]** function key to go to the next Netxport Log Configuration screen. There are a total of six logging configuration screens.

Enable or disable logging classes (or accept HP-recommended defaults). Press the **[Save Data]** key on each screen to create or modify the data record. Verify that the data record has been created by checking that the Data flag is Y.

Fields

`Console Logging` The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to the system console. A value must be entered for each subsystem and class listed. A Y (yes) enables logging to the console, N

(no) disables logging to the console.

`Disk Logging`

The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to a disk file. A value must be entered for each subsystem and class listed. A `Y` (yes) enables logging to a file, `N` (no) disables logging to a file. The file name for the log file is `NMLG`*`nnnn`*`.PUB.SYS`, where *`nnnn`* is a number from *`0000`* to *`9999`*. All logging classes in all subsystems are logged to this file. At each system startup, or when a file is full, the node management services subsystem (NMS) creates a new `NMLG`*`nnnn`*`.PUB.SYS` file, naming each successive logging file by incrementing *`nnnn`*. When `NMLG`*`9999`*`.PUB.SYS` is full, NMS names the next logging file `NMLG`*`0000`*`.PUB.SYS`.

The Netxport Log Configuration (2) screen (#60) in Figure 13-3 is displayed when you press the **[Next Screen]** function key from the Netxport Log Configuration (1) screen (#61) in Figure 13-2.

Figure 13-3 Netxport Log Configuration (2) Screen

```
NMMGR/3000 (V.uu.ff) #60  Netxport Log Configuration (2)              Data: Y
Fill in the required information; then press the Save Data key.
Command:

            Class     Console Disk
Subsystem   Name      Logging Logging  Event

SUB0004     CLAS0000  [N]     [Y]      Notable events
DC/LDM

SUB0005     CLAS0000  [Y]     [Y]      Internal errors
Network     CLAS0001  [N]     [Y]      Resource errors
IPC         CLAS0002  [N]     [N]      Informative messages

SUB0006     CLAS0002  [N]     [Y]      Resource errors
Network     CLAS0003  [Y]     [Y]      Internal errors
Services    CLAS0004  [N]     [Y]      Detailed events (enable with NSCONTROL LOG)
            CLAS0005  [Y]     [Y]      NetIPC internal errors

To enable user logging for a class, press Save Data and then type
"@LOGGING.SUB00xx.CLAS00xx" on the command line and presss ENTER.

To see more logging class options, press the Next Screen key.
File:  NMCONFIG.PUB.SYS
```

Next Screen	Prev Log Screen		Exit Logging		Validate Netxport	Save Data	Help	Prior Screen

Use the fields and the function keys of the screen to configure logging for the subsystems represented on the screen. If the subsystem for which you want to enable logging does not appear on this screen, press the **[Next Screen]** function key to go to the next Netxport Log Configuration screen. There are a total of six logging configuration screens.

Enable or disable logging classes (or accept HP-recommended defaults). Press the **[Save Data]** key on each screen to create or modify the data record. Verify that the data record has been created by checking that the Data flag is Y.

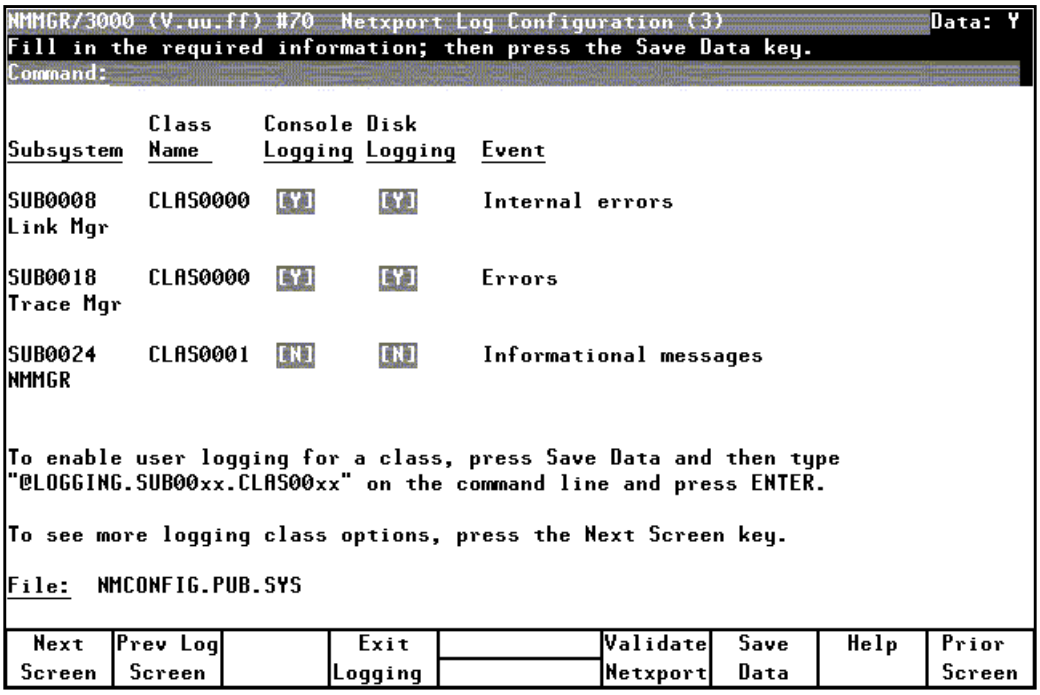
Fields

`Console Logging` — The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to the system console. A value must be entered for each subsystem and class listed. A `Y` (yes) enables logging to the console, `N` (no) disables logging to the console.

`Disk Logging` — The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to a disk file. A value must be entered for each subsystem and class listed. A `Y` (yes) enables logging to a file, `N` (no) disables logging to a file. The file name that NMS uses is `NMLG`*`nnnn`*`.PUB.SYS`, where *`nnnn`* is a number from *`0000`* to *`9999`*. All logging classes in all subsystems are logged to this file. At each system startup, or when a file is full, NMS creates a new `NMLG`*`nnnn`*`.PUB.SYS` file, naming each successive logging file by incrementing *`nnnn`*. When `NMLG`*`9999`*`.PUB.SYS` is full, NMS names the next logging file `NMLG`*`0000`*`.PUB.SYS`.

The Netxport Log Configuration (3) screen (#70) in Figure 13-4 is displayed when you press the **[Next Screen]** function key from the Netxport Log Configuration (2) screen (#60) in Figure 13-3.

Figure 13-4 Netxport Log Configuration (3) Screen



Use the fields and the function keys of the screen to configure logging for the subsystems represented on the screen. If the subsystem for which you want to enable logging does not appear on this screen, press the **[Next Screen]** function key to go to the next Netxport Log Configuration screen. There are a total of six logging configuration screens.

Enable or disable logging classes (or accept HP-recommended defaults). Press the **[Save Data]** key on each screen to create or modify the data record. Verify that the data record has been created by checking that the Data flag is Y.

Fields

`Console Logging` The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to the system console. A value must be entered for each subsystem and class listed. A Y (yes) enables logging to the console, N (no) disables logging to the console.

`Disk Logging` The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to a disk file. A value must be entered for each subsystem and class listed. A Y (yes)

enables logging to a file, N (no) disables logging to a file. The file name that NMS uses is NMLG*nnnn*.PUB.SYS, where *nnnn* is a number from *0000* to *9999*. All logging classes in all subsystems are logged to this file. At each system startup, or when a file is full, NMS creates a new NMLG*nnnn*.PUB.SYS file, naming each successive logging file by incrementing *nnnn*. When NMLG*9999*.PUB.SYS is full, NMS names the next logging file NMLG*0000*.PUB.SYS.

The Netxport Log Configuration (4) screen (#68) in Figure 13-5 is displayed when you press the **[Next Screen]** function key from the Netxport Log Configuration (3) screen (#70) in Figure 13-4.

Figure 13-5 Netxport Log Configuration (4) Screen

```
NMMGR/3000 (V.uu.ff) #68  Netxport Log Configuration (4)              Data: Y
Fill in the required information; then press the Save Data key.
Command:

            Class     Console Disk
Subsystem   Name      Logging Logging  Event

SUB0025     CLAS0001  [N]     [Y]      Errors
ThinLAN     CLAS0002  [N]     [Y]      Warnings
HPPB Link   CLAS0003  [N]     [Y]      Informational messages

SUB0028     CLAS0010  [N]     [Y]      Errors
LAPB PSI    CLAS0012  [N]     [Y]      Informational messages
HPPB Link

SUB0040     CLAS0001  [Y]     [Y]      Catastrophic errors
Remote      CLAS0002  [Y]     [Y]      Serious errors
Link Mgr    CLAS0003  [Y]     [Y]      Notable errors
            CLAS0004  [N]     [Y]      Nodal messages (start/stop)
            CLAS0005  [N]     [Y]      Informative messages

To enable user logging for a class, press Save Data and then type
"@LOGGING.SUB00xx.CLAS00xx" on the command line and press ENTER.
To see more logging class options, press the Next Screen key.
```

Next Screen	Prev Log Screen		Exit Logging		Validate Netxport	Save Data	Help	Prior Screen

Use the fields and the function keys of the screen to configure logging for the subsystems represented on the screen. If the subsystem for which you want to enable logging does not appear on this screen, press the **[Next Screen]** function key to go to the next Netxport Log Configuration screen. There are a total of six logging configuration screens.

Enable or disable logging classes (or accept HP-recommended defaults). Press the **[Save Data]** key on each screen to create or modify the data

record. Verify that the data record has been created by checking that the Data flag is Y.

Press the **[Exit Logging]** function key when you have finished modifying the logging configuration.

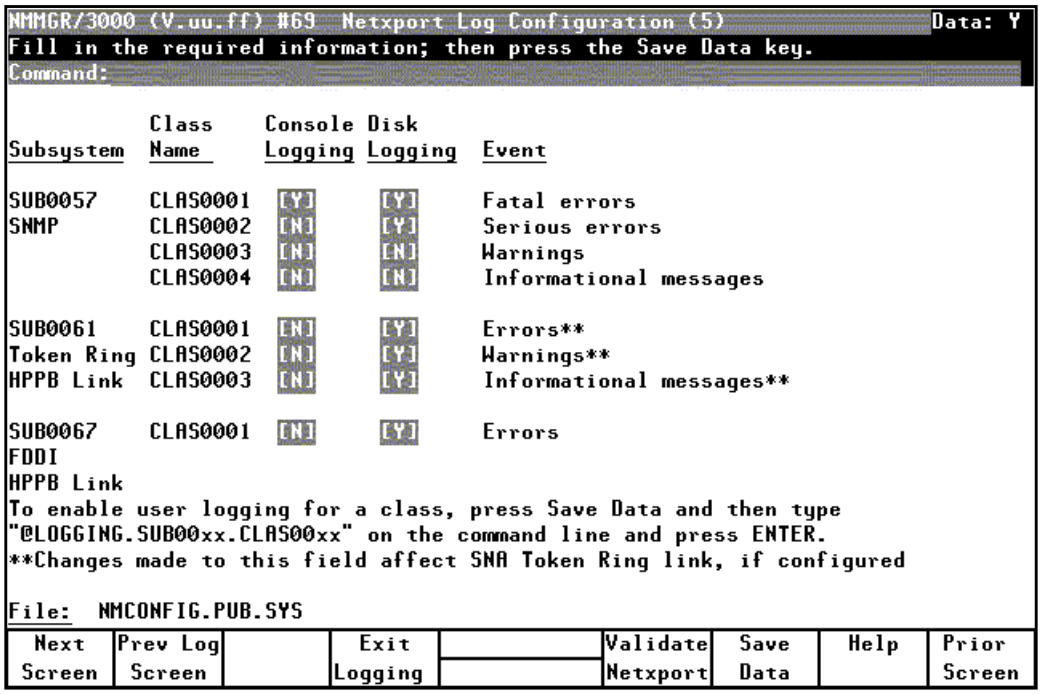
Fields

`Console Logging` — The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to the system console. A value must be entered for each subsystem and class listed. A Y (yes) enables logging to the console, N (no) disables logging to the console.

`Disk Logging` — The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to a disk file. A value must be entered for each subsystem and class listed. A Y (yes) enables logging to a file, N (no) disables logging to a file. The file name that NMS uses is NMLG*nnnn*.PUB.SYS, where *nnnn* is a number from *0000* to *9999*. All logging classes in all subsystems are logged to this file. At each system startup, or when a file is full, NMS creates a new NMLG*nnnn*.PUB.SYS file, naming each successive logging file by incrementing *nnnn*. When NMLG*9999*.PUB.SYS is full, NMS names the next logging file NMLG*0000*.PUB.SYS.

The Netxport Log Configuration (5) screen (#69) in Figure 13-6 is displayed when you press the **[Next Screen]** function key from the Netxport Log Configuration (4) screen (#68) in Figure 13-5.

Figure 13-6 Netxport Log Configuration (5) Screen



Use the fields and the function keys of the screen to configure logging for the subsystems represented on the screen. If the subsystem for which you want to enable logging does not appear on this screen, press the **[Next Screen]** function key to go to the next Netxport Log Configuration screen. There are a total of six logging configuration screens.

Enable or disable logging classes (or accept HP-recommended defaults). Press the **[Save Data]** key on each screen to create or modify the data record. Verify that the data record has been created by checking that the Data flag is Y.

Press the **[Exit Logging]** function key when you have finished modifying the logging configuration.

Fields

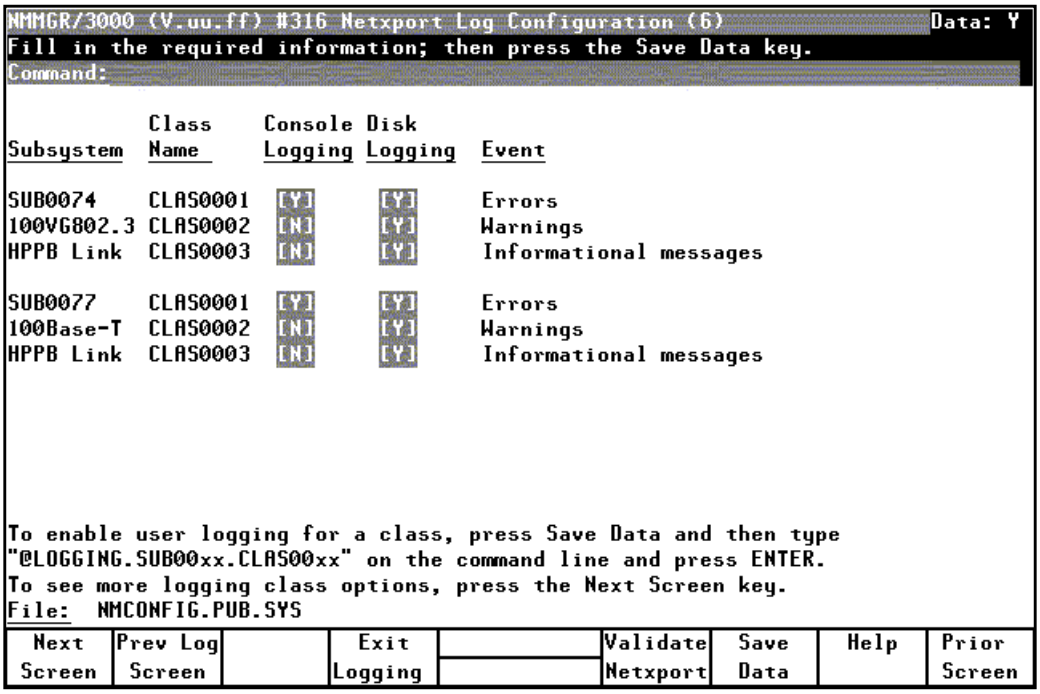
`Console Logging` — The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to the system console. A value must be entered for each subsystem and class listed. A `Y` (yes) enables logging to the console, `N` (no) disables logging to the console.

`Disk Logging` — The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to a disk file. A

value must be entered for each subsystem and class listed. A Y (yes) enables logging to a file, N (no) disables logging to a file. The file name that NMS uses is NMLG*nnnn*.PUB.SYS, where *nnnn* is a number from *0000* to *9999*. All logging classes in all subsystems are logged to this file. At each system startup, or when a file is full, NMS creates a new NMLG*nnnn*.PUB.SYS file, naming each successive logging file by incrementing *nnnn*. When NMLG*9999*.PUB.SYS is full, NMS names the next logging file NMLG*0000*.PUB.SYS.

The Netxport Log Configuration (6) screen (#316) in Figure 13-7 is displayed when you press the **[Next Screen]** function key from the Netxport Log Configuration (5) screen (#69) in Figure 13-6.

Figure 13-7 Netxport Log Configuration (6) Screen



Use the fields and the function keys of the screen to configure logging for the subsystems represented on the screen. If the subsystem for which you want to enable logging does not appear on this screen, press the **[Next Screen]** function key to go to the next Netxport Log Configuration screen. There are a total of seven logging configuration screens.

Fields

Enable or disable logging classes (or accept HP-recommended defaults). Press the **[Save Data]** key on each screen to create or modify the data record. Verify that the data record has been created by checking that the Data flag is Y.

`Console Logging`

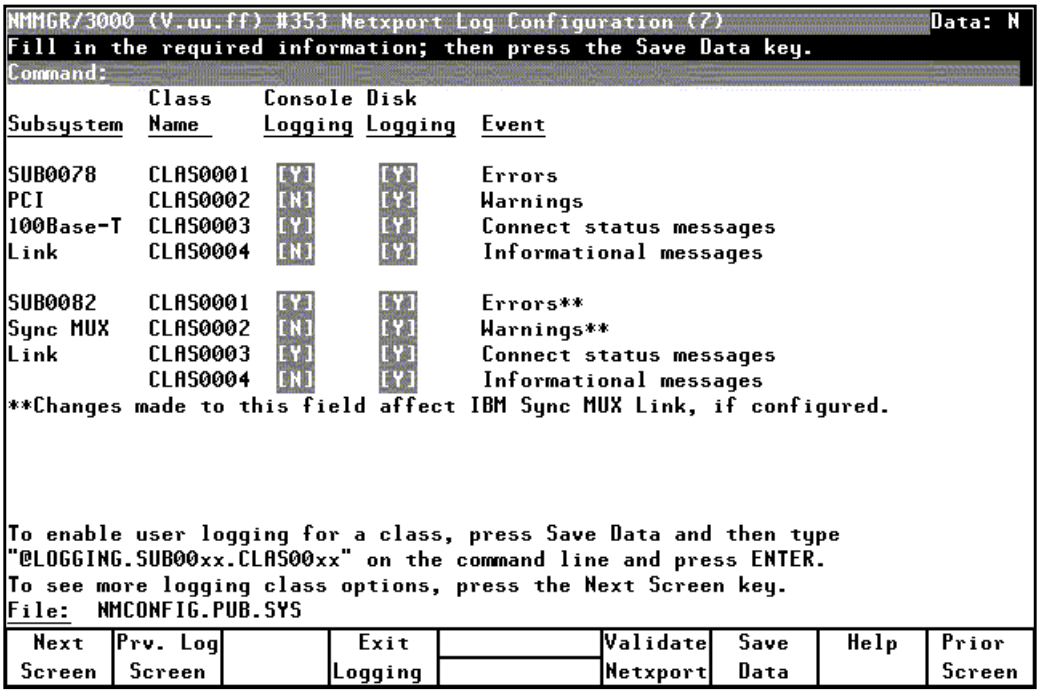
The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to the system console. A value must be entered for each subsystem and class listed. A Y (yes) enables logging to the console, N (no) disables logging to the console.

`Disk Logging`

The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to a disk file. A value must be entered for each subsystem and class listed. A Y (yes) enables logging to a file, N (no) disables logging to a file. The file name that NMS uses is NMLG*nnnn*.PUB.SYS, where *nnnn* is a number from *0000* to *9999*. All logging classes in all subsystems are logged to this file. At each system startup, or when a file is full, NMS creates a new NMLG*nnnn*.PUB.SYS file, naming each successive logging file by incrementing *nnnn*. When NMLG*9999*.PUB.SYS is full, NMS names the next logging file NMLG*0000*.PUB.SYS.

The Netxport Log Configuration (7) screen (#353) in Figure 13-8 is displayed when you press the **[Next Screen]** function key from the Netxport Log Configuration (6) screen (#316) in Figure 13-7.

Figure 13-8 Netxport Log Configuration (7) Screen



Use the fields and function keys of the screen to configure logging for the subsystems represented on the screen. The subsystems 78 (PCI 100Base-T) and 82 (Sync MUX link) can be configured from this screen.

Fields

Enable or disable logging classes (or accept HP-recommended defaults). Press the **[Save Data]** key on each screen to create or modify the data record. Verify that the data record has been created by checking that the Data flag is Y.

Console Logging

The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to the system console. A value must be entered for each subsystem and class listed. A Y (yes) enables logging to the console, N (no) disables logging to the console.

Disk Logging

The value entered in this field specifies whether or not logging events for the subsystem and class listed beside the field will be logged to a disk file. A value must be entered for each subsystem and class listed. A Y (yes) enables logging to a file, N (no) disables logging to a file.

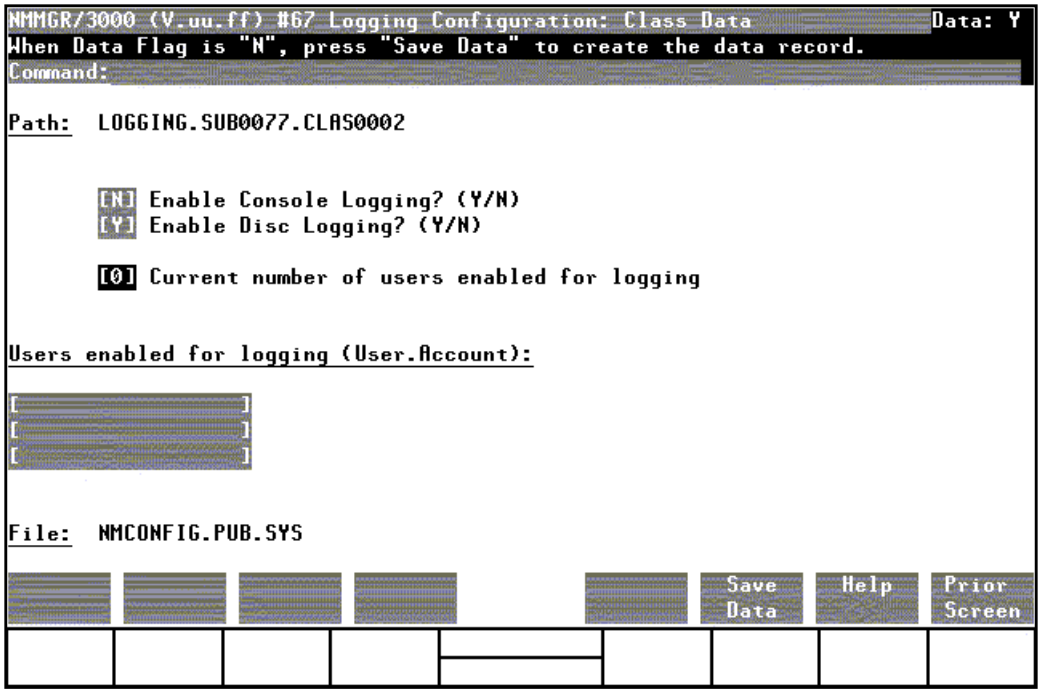
Enable Users for Individual Logging Classes

The logging screens described previously in this chapter make it possible to completely configure logging for all subsystems by traversing only seven screens. However, using these screens, it is not possible to configure logging so that messages generated by specific logging classes are sent to an individual user's list device.

The following steps describe the method used to configure users to receive logging messages. Using this method, you can create a configuration that allows messages from a single logging class, or a set of classes, to be sent to a user's list device.

To do so, you access and update the Logging Configuration Class Data screen (#67) in Figure 13-9, according to the steps that follow.

Figure 13-9 Logging Configuration: Class Data Screen



Step 1. Type the path name:

@LOGGING.SUB*nnnn*.CLAS*nnnn*

in the command window of any screen and press the **[ENTER]** key, where SUB*nnnn* is the subsystem ID and CLAS*nnnn* is the class name of the logging class you want directed to the user's list device.

For example, subsystem 77, class 2 would be entered as:
@LOGGING.SUB0077.CLASS0002

Step 2. To enable console logging for this subsystem logging class, enter a Y in the Enable console logging? field. To disable console logging, enter an N. **Be aware that changing the value in this field will override the previous setting for the logging class you are configuring**.

Step 3. To enable disk logging for this subsystem logging class, enter a Y in the Enable disk logging? field. To disable console logging, enter an N. **Be aware that changing the value in this field will override the previous setting for the logging class you are configuring.**

Step 4. Enter up to three names, in the form user.account, in the Users enabled for logging fields. If these fields already contain names it is because user names were previously configured using this screen. If less than three user names are configured, type the new user name in an empty field. If all fields are used, type over one of the old user names to replace it with the new user name. (Note that the user name you type over will no longer be enabled to receive these logging messages.)

Step 5. Press the **[Save Data]** function key to modify the data record.

Step 6. Press the **[Prior Screen]** key to return to the screen from which you accessed the Logging Configuration: Class Data screen.

Repeat the above procedure for each subsystem logging class for which you want to enable users.

CAUTION Enabling users to receive logging messages can strain system resources. Hewlett-Packard recommends that you use this capability sparingly and only for short periods of time.

Activate Logging

NetIPC logging is automatically activated at system start up. Link manager logging and network transport logging are activated when you initiate the network transport (NETCONTROL START). Network Services logging is activated when the Network Services are initiated (that is, when the NSCONTROL START command is issued).

Network Link logging is activated when the specific link is first started.

When you are changing a logging configuration for a specific subsystem, the changes will normally take effect when you perform a SWITCHNMLOG UPDATE command. In some cases, however, such as when no logging is currently active, the subsystem may need to be deactivated and restarted. The steps that must be taken for each subsystem are shown in Table 13-1.

Table 13-1 Subsystem Activation/Deactivation

Subsystem	Steps
Network Transport	NETCONTROL STOP (if already active) NETCONTROL START
NetIPC (sockets)	NETCONTROL STOP (if already active) NETCONTROL START NETCONTROL UPDATE
Network Services	NSCONTROL STOP (if already active) NSCONTROL START
Link Manager	NETCONTROL STOP (if already active) SNACONTROL STOP;node=nodename (refer to the *SNA Link/XL Node Manger's Guide*) SNACONTROL START;NODE=nodename NETCONTROL START
Link Logging (non-DTS)	NETCONTROL STOP; NET = niname (if already active) NETCONTROL START; NET = niname
Link Logging (DTS link)	Restart the system or use :DTCCNTRL option 4 (shutdown) followed by option 5 (restart).

How to use the log messages for troubleshooting is described in the *NS 3000/iX Error Messages Reference Manual*. How to format the log file for examination is described in *Using the Node Management Services (NMS) Utilities*.

14 Operating the Network

After you have completed the configuration process, you are ready to activate NS. This chapter shows you how to bring up an NS 3000/iX node and how to shut it down. It assumes you have successfully completed the configuration steps described previously.

For more detailed information on starting, stopping, and operating an NS network, see the *NS 3000/iX Operations and Maintenance Reference Manual*.

This chapter includes step-by-step instructions to help you perform the following tasks:

- Start links and services.
  - — Start software loopback (optional).
  - — Start the links.
  - — Start Network Services.
- Test Network Services.
- Shut down links and services.

Start Links and Services

Start Software Loopback

Issue the following command (NM capability required) to start software loopback:

```
NETCONTROL START;NET=loopbackNIname
```

This starts up the control process, the transport, and software loopback. Note: when you use guided NMMGR to create any NI, a loopback network interface (whose `loopbackNIname` is `LOOP`) is automatically generated. The loopback NI must be started if you wish to perform local loopbacks or to `DSLINE` to the local node, also some ARPA services need loopback to be started.

Start a Link

Issue the following command (NM capability required) to start a link:

```
NETCONTROL START;NET=NIname
```

This starts the link identified by the NI name. (If no previous `NETCONTROL START` command was issued, then the control process and transport are also started.) The `NIname` is the network interface (NI) name that you supplied during NS configuration. You can start the link before loopback if you want. Start other links as needed.

Start a Host-Based X.25 Link

If your network includes X.25 links and you are using host-based network management, you will need to use the `DTCCNTRL` command *before* you issue the `NETCONTROL START` command. `DTCCNTRL` starts X.25 and PAD support for the DTC/X.25 Network Access card. Issue the following command (System Operator capability required):

```
DTCCNTRL DTC=dtcname;CARD=cardnumber;FUNC=function
```

where `function` is one of the following:

`STARTX25` to start X.25 services;

`STARTPADSUP` to start PAD support services;

`STARTBOTH` to start both X.25 and PAD support services.

For more information on starting host-based X.25 links as well as other uses of the `DTCCNTRL` command, see *Configuring and Managing Host-Based X.25 Links*.

NOTE If you are starting an X.25 link for a system using PC-based network management or if you are not starting an X.25 link, you do not need to use the DTCCNTRL command.

Start Network Services

Issue the following command (NM capability required) to start the network services:

```
NSCONTROL START
```

This starts the NS 3000/iX Network Services, such as Virtual Terminal, Network File Transfer, Remote File Access, and Remote Data Base Access.

You may want to create a startup UDC or command file to activate software loopback, the link(s), and the network services. If you do so, you must separate each command with a brie pause to allow for processing (rxample: “:PAUSE 5”).

Test Network Services

In order to test that you have successfully configured and brought up your NS node, HP provides an NS validation test called QVALNS.NET.SYS. QVALNS is a program which modifies a file called TQVALNS and streams it as a temporary job (JQVALNS). The job purges and creates various files, and then runs a program called NSTEST. NSTEST tests the network services (VT, RFA, RDBA, and NFT).

To run the NS validation test, follow the step below:

Step 1. Run the NS validation test on your own node. This tests the software loopback capability. Issue the following command, where node is the node portion of your own node name:

```
RUN QVALNS.NET.SYS;INFO=node
```

Step 2. Run the NS validation test on another system on the same network. Select a remote node on the network and make sure that the link and the network services are up on the remote system by issuing the following commands on that node (NM capability required):

```
NETCONTROL STATUS
```

```
NSCONTROL STATUS
```

If the link or network services have not been started, either pick another node or start them.

Note the node name of the remote node (given in the last line of output from the NETCONTROL STATUS command). If you followed the configuration steps in this manual, the second and third portions of the node name (the domain and organization) should be the same as the second and third portions of the local node.

Step 3. Run the NS validation test across the link by issuing the following command at the local node, where node is the node portion of the remote node name:

```
RUN QVALNS.NET.SYS;INFO=node
```

If you encounter problems, see the *NS 3000/iX Operations and Maintenance Reference Manual* and to the *NS 3000/iX Error Messages Reference Manual* for information on diagnostics and troubleshooting.

Shut Down Network Services

To shut down NS, issue the following commands (NM capability required):

```
DSLINE @;CLOSE

NSCONTROL STOP

NETCONTROL STOP
```

The DSLINE command shown above closes connections for your session only.

NSCONTROL STOP allows existing users to continue using the services until they finish their current task but prevents new uses of the services by these users or by new users. Therefore, the services are not actually stopped until all existing users finish using them. You can use NSCONTROL ABORT instead if you wish to immediately terminate all use of the services.

NETCONTROL STOP closes all open connections. To determine if there are any sessions still active, enter: NSCONTROL STATUS. If you do not want to wait until existing users are finished with their current tasks before you bring down the system, issue NSCONTROL ABORT and then NETCONTROL STOP.

If a host-based X.25 link is started, you will also need to issue a DTCCNTRL command to stop X.25 and PAD support for the DTC/X.25 Network Access card. Enter the DTCCNTRL command after the NSCONTROL STOP and NETCONTROL STOP commands. Enter the command as:

```
DTCCNTRL DTC=dtcname;CARD=cardnumber;FUNC=function
```

where function is one of the following:

STARTX25	to start X.25 services;
STARTPADSUP	to start PAD support services;
STARTBOTH	to start both X.25 and PAD support services.

A MPE/V to MPE/iX Migration

This appendix provides a quick overview of the planning and tasks you will need to do to migrate an NS 3000 network from an MPE/V system to an MPE/iX system. This appendix assumes that you are migrating your network as a whole; that is, replacing all MPE V systems with MPE/iX systems and maintaining the same basic network function.

The following topics are covered by this appendix:

- Differences between NS 3000/V and NS 3000/iX networks.
- An overview of migration tasks.
- Guidelines for converting files.
- Guidelines for reconfiguring a network.

NOTE For information on migrating X.25 links, refer to the remaining appendixes of this manual.

Differences Between NS 3000/V and NS 3000/iX

There are a number of differences between the way NS is implemented on MPE V systems and the way it is implemented on MPE/iX systems. These differences affect the network itself, some of the applications that users may run over the network, and the command used to obtain status information about the network. Since it is helpful to understand these differences as you prepare to move an existing MPE V network to MPE/iX, they are summarized below.

Network

A number of the methods available for making connections to an MPE V network are not available with NS 3000/iX. If your MPE V network includes one of these you will need to modify your network configuration before attempting to use the network on MPE/iX systems. More information on the specific steps required to modify or remove unsupported links or connections can be found later in this appendix.

The connection methods that are not supported on NS 3000/iX are:

- Manual dial modems.
- Asynchronous Network Link.
- Bisynchronous link-level protocol.

In addition, while it is possible to access a DS/3000 node directly from an NS 3000/V node, this capability is not supported on NS 3000/iX. A user of an NS 3000/iX network who wants to access a DS/3000 node must first access an MPE V NS node. This is because the DS/3000 code that was included as a subset of the NS 3000/V code is not provided with NS 3000/iX.

Configuration Files

NS 3000/V network configuration files are separated into two files, the `NMCONFIG` file, which contains link information, and the `NSCONF` file, which contains the transport configuration and other subsystems you have purchased such as SNA.

NS 3000/iX systems have a single `NMCONFIG.PUB.SYS` file that contains information for the network transport, for NetIPC and link-level logging, and also for the Datacommunications and Terminal Subsystem (DTS). `NMCONFIG.PUB.SYS` also contains information for any other subsystems you have purchased such as SNA.

Applications Support

There are also differences in the implementations of NS 3000/V and NS 3000/iX that will affect certain applications that users may currently be running on your MPE V network. These differences are as follows:

- NS 3000/iX supports PTOP for HPDESK only.

  On NS 3000/iX PTOP is not supported for applications other than HPDESK. Network users who are running PTOP programs will need to convert them to NetIPC/RPM or BSD programs before running them on an NS 3000/iX network. Refer to the *NetIPC 3000/XL Programmer's Reference Manual* and the *Using NS 3000/iX Network Services* for more information.

- Nowait I/O RFA is not available with NS 3000/iX.

  Privileged mode programs that use nowait I/O Remote File Access over an MPE V network will need to be modified before they can be run on an NS 3000/iX network. Refer to the *Using NS 3000/iX Network Services* for more information.

Obtaining Status Information

On MPE V systems the `SHOWCOM` command returns status information about a communication device, and is used to determine line activity and quality. This information is still available on NS 3000/iX, but is accessed through a different command. Use the `LINKCONTROL STATUS` command to access status information on NS 3000/iX.

Migration Overview

There are a number of steps that you must take to successfully convert an MPE V network for use as an MPE/iX network. These tasks are summarized below, and described in more detail in the remainder of this appendix. Keep in mind that, depending on the needs of your installation, you may need to perform additional tasks to complete your migration. For example, if you are adding communication links that did not exist on your MPE V network you will also need to configure those new links.

Before You Start

This guide provides an extensive overview of NS architecture and networking concepts. It also furnishes configuration design checks, planning worksheets and examples to aid you in organizing new network configurations. You should be thoroughly familiar with this material before you begin your migration.

File Migration Tasks

There are two primary tasks you will need to perform to migrate your network configuration files. These are:

1. Run the NMMGRVER utility on the old configuration files to convert them to the current software version. (You will first need to install a copy of all configuration files used for your NS 3000/V network to the MPE/iX network). Refer to “File Conversion Guidelines” later in this Appendix.
2. Run the NMMGR utility on the new configuration file(s) to make any changes required due to the differences between NS 3000/V and NS 3000/iX. Refer to “Reconfiguration Guidelines” later in this Appendix.

Additional Migration Considerations

This appendix does not discuss hardware migration considerations; however, you will find a description of hardware components in this manual. Additionally, details of hardware installation and configuration can be found in the following manuals:

- *LANIC Installation and Service Manual.*
- *LAN Cable and Accessories Installation Manual.*
  - *Central Bus Programmable Serial Interface Installation and Reference Manual.*

File Conversion Guidelines

A file conversion utility called NMMGRVER.PUB.SYS allows you to convert earlier versions of subsystems for use with the current version of Node Management Services (NMS) by converting the files to an acceptable format.

When to Convert Files

If you have not successfully converted your files you will be notified that conversion is necessary when you try either to run NMMGR or to perform a NETCONTROL command. If you attempt to run NMMGR against an unconverted configuration file you will receive the message:

```
Version mismatch found on specified subsystem. Please run
NMMGRVER. (NMGRERR 53)
```

If you attempt to perform NETCONTROL while using unconverted files you will receive the following message at the console:

```
Bad CONFIG File Version
```

In either case you should stop your current activity and run the NMMGRVER.PUB.SYS file conversion utility on your configuration files.

WARNING **The conversion procedure that follows will not preserve any previously configured Distributed Terminal Subsystem (DTS) configuration values. If you are updating from an earlier version of MPE/iX at the same time you are migrating from NS 3000/V to NS 3000/iX, you should see the information under "Updating From a Previous MPE/iX Version" later in this Appendix before converting your configuration files.**

Converting Files

Follow these steps to convert configuration files using NMMGRVER:

Step 1. Make a backup copy of the existing configuration files.

Step 2. Install a copy of the MPE/V NMCONFIG file to NMCONFIG.PUB.SYS on the MPE/iX system, and then install copies of any NSCONF files.

Step 3. Execute NMMGRVER.PUB.SYS by entering:

```
RUN NMMGRVER.PUB.SYS
```

The system responds with the following banner:

NMS Configuration File Conversion Utility 32099-11018 V.uu.ff (C) Hewlett-Packard Co. 1985

Step 4. The system will then prompt for the name of the configuration file to be converted by displaying the message:

```
Fileset to be scanned?
```

You can then choose to end the conversion program by pressing the **[RETURN]** key, or you can enter one of the following filesets:

```
filename [.groupname [.acctname]]
```

```
@ [.groupname [.acctname]]
```

```
@.@ [.acctname]
```

```
@.@.@
```

NMMGRVER searches for files of type `nconf` in the specified fileset. For each file found, it asks:

```
OK to convert filename.groupname.acctname?
```

where `filename.groupname.acctname` is the name of a configuration file. Enter `Y` for yes, or enter either `N` or **[RETURN]** for no.

Step 5. NMMGRVER checks the configuration file to determine whether it is an MPE/V or an MPE/iX configuration file. If it is an MPE/iX file the conversion proceeds without further user input. If the file is an MPE/V file, however, NMMGRVER prompts you for the type of MPE/V file you are converting, as follows:

```
What is the type of this file?

   1) MPE V NSCONF
   2) MPE V NMCONFIG
   3) skip this file

Enter a value between 1 and 3.
```

Enter the appropriate value.

Step 6. After each file is converted NMMGRVER will display the following message:

```
FILE CONVERTED
```

Continue to enter either `Y`, `N`, or **[RETURN]** until you have converted all files.

In the conversion process, NMMGRVER will merge the information from each `NSCONF` file accepted for conversion with `NMCONFIG.PUB.SYS`, and create new (converted) `NSCONF` files. If you have converted more than one `NSCONF` file, you will need to choose the file that corresponds to the network configuration you want, and rename it as the new `NMCONFIG.PUB.SYS`. Choose the `NSCONF` file that corresponds to the network configuration you want to use as your NS 3000/iX configuration.

This new NMCONFIG.PUB.SYS file contains your NS configuration in a format acceptable to MPE/iX. You can now run NMMGR to configure the DTS subsystem, and to perform any needed modifications to the NS configuration. See “Reconfiguration Guidelines” later in this appendix.

Updating From a Previous MPE/iX Version

Updating from an earlier version of MPE/iX at the same time migrating from NS 3000/V to NS 3000/iX, you will need to make a choice between reconfiguring Distributed Terminal Subsystem (DTS) and reconfiguring the NS network. The choice is necessary because MPE/V versions of NMCONFIG.PUB.SYS files do not include DTS configuration values.

The circumstances of the installation determine which configuration values to preserve. If the NS network is complex, you may decide to convert the existing MPE/V configuration files, and reconfigure DTS. In this case you should follow the steps under “File Conversion Guidelines” earlier in this appendix.

If, on the other hand, your DTS configuration is extensive, you may decide to migrate your existing MPE/iX configuration files to the new version of MPE/iX. You will then need to redo your NS network configuration so that both the NS and DTS configurations are contained in a single, valid, MPE/iX NMCONFIG.PUB.SYS file. In any case, you will need to reconfigure either NS or DTS if you are both updating MPE/iX and converting from an NS 3000/V network to an NS 3000/iX network.

Reconfiguration Guidelines

Once the MPE/V NS configuration files have been converted for use with the MPE/iX version of NS, reconfigure your network to account for the implementation differences between NS 3000/V and NS 3000/iX. Run the NMMGR utility against the configuration file generated by the file conversion process and perform the following reconfiguration tasks:

- Configure the physical path of all links for your network. This configuration consists of a channel number (CCC) and subchannel number (SSS) in the form CCC.SSS. There is no channel or subchannel associated with NS on MPE V.
- Since the LAP-B protocol is the only point-to-point link-level protocol supported on the MPE/iX computer, you must reconfigure links that were configured as bisynchronous links on NS 3000/V as LAP-B links, or remove them from the network configuration.
- Configure the Distributed Terminal Subsystem (DTS) according to the needs of your installation. Refer to *Configuring Systems for Terminals, Printers, and Other Serial Devices* for instructions on how to configure the DTS.

The above configuration tasks are a general summary of what you will need to do to reconfigure your network to run on MPE/iX. You should be aware that there are many changes to individual screens and screen fields. Refer to this guide for information on individual screens and screen fields.

B NS X.25 Migration: NS 3000/V to NS 3000/iX

This Appendix tells how to use the NMMGRVER utility to migrate (update) configuration files from a node running NS X.25 3000/V Link to a node that will be running NS 3000/iX release 2.0 or later. This appendix does *not* apply if an MPE V based node is being used as an X.25 server for NS 3000/XL based machines. Refer to the following appendixes depending on which X.25 network products you currently have:

- Migrating a configuration file from a node running NS 3000/V PAD to an NS 3000/iX node that will be running NS 3000/iX release 2.0 or later, refer to Appendix C , “NS X.25 Migration: NS 3000/V PAD Access to NS 3000/iX.”

This Appendix also provides an overview of the differences between networking functionality on an MPE V and an MPE/iX system you need to consider for migration.

Differences Between NS 3000/V and NS 3000/iX

The following paragraphs summarize differences between NS 3000/V and NS 3000/iX. Make sure that you account for these differences that could affect your network when migrating to NS 3000/iX. For information on operating system migration, refer to the MPE/iX Migration series.

Hardware

Some NS 3000/V hardware components are not part of an NS 3000/iX network, such as the ATP for terminal connections, and the INP for network links.

On an NS 3000/iX network, the DTC provides connections for local or remote terminals and serial printers. The DTC also provides MPE/iX access to X.25 through a DTC/X.25 Network Access card. The Datacommunications and Terminal Subsystem (DTS) LANIC on the MPE/iX host is used for system-to-system X.25 connectivity.

Unsupported Network Connections

Before migrating your network, identify any unsupported network connections. The network connections that are not supported on NS 3000/iX networks are as follows:

- Manual-dial modems.
- Asynchronous SERIAL Network Link and bisynchronous link-level protocol. To ease migration, you can convert Asynchronous SERIAL network links to the NS 3000/V Point-to-Point links which can be converted to NS 3000/iX. Point-to-Point links use the LAP-B protocol.
- Connections to DS/3000 nodes. DS network services are not supported on NS 3000/iX. If DS/3000 nodes are part of an existing network, either migrate them to NS 3000/V or maintain NS 3000/V connections to the DS/3000 nodes.

Configuration of Terminals and Printers

On NS 3000/V networks, the `SYSDUMP` program is used to perform I/O configuration which includes configuring terminals, printers, and other I/O devices and drivers. On NS 3000/iX, terminals and serial printers are configured on the host (using NMMGR) and on the OpenView Windows Workstation (using the OpenView DTC Manager software). For more information on configuration using your OpenView Windows Workstation, read *Using the OpenView DTC Manager*.

PAD devices on NS 3000/V are configured (using NMMGR) as part of the X.25 network configuration. On NS 3000/iX when PC-based network management is used, PAD devices are configured both on the host (using NMMGR) and on the OpenView Windows Workstation (using the OpenView DTC Manager software).

Configuration Files

NS 3000/V network configuration files are separated into two files, the `NMCONFIG` file, which contains link information, and the `NSCONF` file, which contains the transport configuration and other subsystems you have purchased such as SNA.

NS 3000/iX systems have a single `NMCONFIG.PUB.SYS` file that contains information for the network transport, for NetIPC and link-level logging, and also for the Datacommunications and Terminal Subsystem (DTS). `NMCONFIG.PUB.SYS` also contains information for any other subsystems you have purchased such as SNA.

Network Services

Differences in the support of network services between NS 3000/V and NS 3000/iX can affect applications that users may currently be running on the NS 3000/V network. These differences are:

- NS 3000/iX supports PTOP for HPDESK only. Network users who are running PTOP programs will need to convert them to NetIPC/RPM programs before running them on an NS 3000/iX network. Refer to the *NetIPC 3000/XL Programmer's Reference Manual* and the *Using NS 3000/iX Network Services* for more information.
- Nowait I/O RFA is not available with NS 3000/iX. Privileged mode programs that use nowait I/O Remote File Access over an NS 3000/V network will need to be modified before they can be run on an NS 3000/iX network. Refer to *Using NS 3000/iX Network Services* for more information.

Obtaining Device Status Information

On MPE V systems, the `SHOWCOM` command returns status information about communication devices such as Local Area Network Interface Controllers (LANICs). On NS 3000/iX systems, this information is available with the `LINKCONTROL...;STATUS` command.

Differences in X.25 Support

There are differences in X.25 support between NS 3000/V and NS 3000/iX which need to be considered when you migrate as described in the following paragraphs.

1980 Versus 1984 CCITT

NS 3000/V supports CCITT 1980 and NS 3000/iX supports both 1980 and 1984.

General Level 3 Differences

In MPE V X.25, a Reset *is* sent to initialize or clear a Permanent Virtual Circuit. In MPE/iX X.25, a Reset *is not* sent to initialize or clear a Permanent Virtual Circuit.

MPE V X.25 has a timeout on an interrupt collision. MPE/iX X.25 does not.

Level 3 Access with NetIPC

In addition to the X.25 features supported on NS 3000/V, NetIPC 3000/XL provides the following CCITT 1984 features:

- Fast select facility.
- The capability of modifying and reading the facility field in call packets.
- A new option in `IPCDEST` (called the destination network address option) allows you to directly specify an X.25 address or PVC number instead of a remote node name. See the *NetIPC 3000/XL Programmers Reference Manual* for more information. If using this feature, you can configure `POOL` as an X.25 Address Key with its security option set to "O" (outbound) in the X.25 SVC Address Key Paths screen to allow outbound calls to any destination address.
- `IPCCONTROL request` 12, reason for error or event, on NS 3000/V can return 14 (network shutdown), 15 (restart sent by local network), 16 (level 2 failure), 17 (restart sent by local protocol module), and 18 (restart packet received). `IPCCONTROL` on NS 3000/XL only returns 10 (Clear), 11 (Reset), or 12 (Interrupt).
- In NS 3000/V, `IPCSHUTDOWN` does not complete until a clear confirmation arrives. In NS 3000/XL, `IPCSHUTDOWN` completes immediately.
- In NS 3000/V, `IPCCREATE` requires that the network name be padded with nulls. In NS 3000/XL, `IPCCREATE` requires the network name be

padded with blanks.

Facilities

The supported facilities of the DTC/X.25 XL Network Link are shown in Table B-1.

Table B-1 Supported Facilities

Supported Facilities	1984 CCITT X.25 Reference
Extended packet sequence number	6.2
Incoming calls barred	6.5
Outgoing calls barred	6.6
Nonstandard default packet size	6.9
Nonstandard default window size	6.10
Flow control parameter negotiation	6.12
Throughput class negotiation	6.13
Closed user group selection (1980 CCITT)	6.14
Fast select request and acceptance	6.16–17
Reverse charging and acceptance	6.18–19
Local charging prevention	6.20
Hunt group	6.25
Supported Facilities with X.25 Level 3 Programmatic Access	
Closed user group related facilities	6.14
Bilateral closed user groups	6.15
Network user identification	6.21
Called line modified address notification	6.26
Call redirection and notification	6.25–27
Transit delay selection and indication	6.28

Security

When configuring a host, you can now set security for each remote system using the Security field on the X.25 SVC Address Key Paths screen. System to System Local User Groups (LUGs) are now assigned on the DTC instead of on the host. The LUG provides security in the same way a CUG does, but you don't have to subscribe to a CUG.

Pad Support

For complete information on migrating PAD support from NS 3000/V to NS 3000/iX Release 2.0 or later, refer to Appendix C , “NS X.25 Migration: NS 3000/V PAD Access to NS 3000/iX.”

Converting NS 3000/V Configuration Files to NS 3000/iX

The procedures that follow are for updating (migrating) configuration files from a node running NS X.25 3000/V Link to a node that will be running NS 3000/iX release 2.0 or later. This conversion procedure can be used with NS 3000/V NMCONFIG and NSCONF files for version V-delta 3 or later. When updating a node running NS X.25 3000/V Link, all NS 3000/V LAN, Point-to-Point, or NRJE as well as X.25 information will be updated to work with MPE/iX.

NOTE The procedures that follow assume that there is no existing NS 3000/XL NMCONFIG file.

Deleting Secondary NIs

If you are migrating from NS X.25 3000/V (release V delta 7 or later) to NS 3000/iX release 2.2 or later, make a backup copy of your NS 3000/V NSCONF file. To migrate to NS 3000/iX release 2.2 or later, you must delete the secondary NIs in the NS 3000/V NSCONF file before you use NMMGRVER to convert it.

Saving NS 3000/V X.25 Parameters

Make a list of the following NS 3000/V parameters that must be re-entered on the DTC.

- VC Assignment from the NS 3000/V screen with the path:

`@NETXPORT.NI.`*`niname`*`.PROTOCOL.X25.VCSPEC`

- X.25 Network type and Flow Control parms from the NS 3000/V screen with the path:

`@NETXPORT.NI.`*`niname`*`.PROTOCOL.X25.VCSPEC. FLOWCNTL`

- L.U.G. Incoming Calls from the NS 3000/V screen with the path:

`@NETXPORT.NI.`*`niname`*`.PROTOCOL.X25.LUGSPEC. INLUG`

- L.U.G. Outgoing Calls from the NS 3000/V screen with the path:

`@NETXPORT.NI.`*`niname`*`.PROTOCOL.X25.LUGSPEC. OUTLUG`

Copying NS 3000/V Configuration Files to NS 3000/iX System

Restore the NS 3000/V configuration files to the NS 3000/iX system. Name the NS 3000/V files with the same names they had on the NS 3000/V node, that is, `NMCONFIG.PUB.SYS`, and if present, `NSCONF.PUB.SYS`.

Remember: This procedure assumes that there is no configuration file on the NS 3000/iX node yet.

Using NMMGRVER

To use the NMMGRVER utility to convert your NS 3000/V configuration file to NS 3000/iX release 2.0 or later, proceed as follows:

Step 1. At the MPE/iX prompt, type: `NMMGRVER.PUB.SYS` and answer the questions.

Step 2. Do either steps a through c or steps d through g.

If your NS 3000/V node had only an `NMCONFIG` file (but no `NSCONF` files), follow the instructions in steps a through c.

a. To convert the `NMCONFIG` file enter the file name: `NMCONFIG.PUB.SYS`.

b. Enter `Y` to proceed when prompted.

c. Select type `2` for `NMCONFIG` type file. The converted file will be saved with the file name you entered. In this case it is `NMCONFIG.PUB.SYS`. This is the only filename that the node will recognize as its configuration file.

If your NS 3000/V node had one or more `NSCONF` files, follow the instructions in steps d through g.

d. Merge your NS 3000/V `NSCONF` file with the NS 3000/V `NMCONFIG` file, and convert it for use with NS 3000/iX release 2.0 or later by entering a file name, for example: `NSCONF1.PUB.SYS`.

e. Enter `Y` to proceed when prompted.

f. Select type `1` for `NSCONF` type file. NMMGRVER will merge the contents of the existing `NMCONFIG` file with the `NSCONF` file you specified. It will be saved in the `NSCONF` file you specified. In this example, `NSCONF1`.

g. If you converted more than one `NSCONF` file, decide which one will be the network configuration you want on the NS 3000/iX system. Rename the file to `NMCONFIG.PUB.SYS`.

Updating X.25 XL System Access Parameters

On the NS 3000/iX host, use NMMGR to change the following parameters to provide X.25 XL System Access:

1. If migrating from any NS 3000/V release before release V delta 7, modify the screen at path `@NETXPORT.NI.`*`niname`*`.PROTOCOL.X25` to change the inactivity timer from minutes to seconds.
2. On the screen with the path `@LINK`, verify that the `DTSLINK` is defined.

3. On the screen with the path @LINK.DTSLINK, verify that the physical path is correctly defined.
4. On the screen with the path @LINK, add the LINK name and Type (X25) of the X25 link. **Note: to migrate to NS 3000/iX release 2.2 or later, repeat this step and steps 5 through 7 for each DTC/X.25 Network Access card.**
5. On the screen with the path @LINK.*linkname*, where the LINK name is the one added in the previous step, add the DTC Node name and card number for the DTC/X.25 Network Access card.
6. On the screen with the path @NETXPORT.NI.*niname*.LINK, add the LINK name entered in Step 4.
7. On the screen with the path @NETXPORT.NI.*niname*.LINK.*linkname*, answer yes or no to start device on network initalization (default is yes) then, press the Update key.

Saving X.25 XL System Access Parameters

Make a list of the following X.25 XL System Access Parameters on the host that must be re-entered under OpenView DTC Manager.

- Local Node Name.
- Link Name (the X25 link, *not* the DTSLINK).
- DTC Node Name.
- DTC Card Number.
- X.25 User Facility Set Parameters.
- SVC and/or PVC numbers for each reachable node.

Adding Other Link Types

For LAN and Point-to-Point link types, run NMMGR and see other sections of this manual for the correct values to be entered.

Verifying DTS Configuration

If the datacommunications and terminal subsystem (DTS) has not been configured, configure the DTS parameters on the host according to the requirements of your network. For more information, refer to *Getting Started with the DTC* and *Configuring Systems for Terminals, Printers, and Other Serial Devices* if you are using PC-based network management. Refer to *Configuring and Managing Host-Based X.25 Links* if you are using host-based network management.

Configuring the DTC

If you are using PC-based network management, configure the DTC by using the OpenView DTC Manager at your OpenView Windows Workstation. For full details, see *Using the OpenView DTC Manager*.

If you are using host-based network management, configure the DTC using NMMGR. For full details, see *Configuring and Managing Host-Based X.25 Links*.

C NS X.25 Migration: NS 3000/V PAD Access to NS 3000/iX

This Appendix tells how to migrate NS 3000/V versions of PAD access to NS 3000/iX release 2.0 or later. For information on migrating X.25, refer to the following appendices, depending on which network configuration you have.

- Migrating a configuration file from a node running NS X.25 3000/V Link to a node that will be running NS 3000/iX release 2.0 or later, refer to Appendix B , “NS X.25 Migration: NS 3000/V to NS 3000/iX.”

PAD Support: NS 3000/V and NS 3000/iX

The following paragraphs summarize differences between NS 3000/V and NS 3000/iX PAD support. You must consider these differences when migrating to NS 3000/iX. For system migration issues, refer to the MPE/iX Migration series for more information.

- PAD facility sets are not supported on NS 3000/iX.
- The packet sizes supported on NS 3000/iX are 128, 256, and 512.
- NS 3000/V PAD sends PAD calls to socket #2563. NS 3000/iX PAD sends PAD calls to the catch-all socket.
- The NS 3000/iX PAD configuration and communication path is different than NS 3000/V. See the migration procedures later in this appendix for details.

Migrating from NS 3000/V PAD Access to NS 3000/iX

There is no conversion tool for migrating NS 3000/V PAD access to NS 3000/iX Release 2.0 or later.

The tasks you must do in order to migrate from NS 3000/V PAD access to NS 3000/iX release 2.0 or later are as follows:

1. Make sure you have accounted for the differences that could affect your network as described in the previous sections of this appendix.
2. Make a list of the NS 3000/V PAD data that must be re-entered for the DTC. Refer to the section in this appendix called “To Save NS 3000/V PAD Parameters.”

Using Host-Based Network Management

1. Use NMMGR to configure DTS parameters on the host.
2. Complete PAD configuration using NMMGR. For complete information on this, see *Configuring and Managing Host-Based X.25 Links*.
   - Remove PAD terminals from the NS 3000/V network directory.

Using PC-Based Network Management

1. Use NMMGR to configure DTS parameters on the host. For complete information on this, read *Configuring Systems for Terminals, Printers, an Other Serial Devices*.
2. Make a list of the DTS parameters configured on the host that must also be entered into the OpenView DTC Manager. Refer to the section in this appendix called “To Save DTS Parameters on the Host.”
3. Configure the DTC by using the OpenView DTC Manager at your OpenView Windows Workstation.
   - Remove PAD terminals from the NS 3000/V network directory.

Saving NS 3000/V PAD Parameters

Make a list of the following NS 3000/V parameters that must be re-entered on the DTC:

- PAD device X.25 addresses fro the NS 3000/V screen with the path: `@NETXPORT.NI.niname.PROTOCOL.X25.SVCPATH`

- L.U.G. Inbound Address from the NS 3000/V screen with the path: `@NETXPORT.NI.niname.PROTOCOL.LUGSPEC.INLUG`
- L.U.G. Outbound Address from the NS 3000/V screen with the path: `@NETXPORT.NI.niname.PROTOCOL.X25.LUGSPEC. OUTLUG`

PAD Access Migration Categories

The way you assign a PAD device depends on what the device is and how it will be used. Asynchronous devices attached to DTCs can either be configured with nailed or non-nailed logical device numbers on each of the MPE/iX host systems to which they have access. The following subsections describe the characteristics of nailed and non-nailed devices.

Non-Nailed Devices

A non-nailed device is a session-accepting device that is not permanently associated with an ldev number at configuration time. When the user at such a device logs on to an MPE/iX system, an ldev is assigned from a pool of ldevs set aside for this purpose at configuration time. The device characteristics of the PAD devices must match the non-nailed PAD terminal profile.

The association between a non-nailed device and the assigned ldev exists only for the duration of the session. One advantage of the use of non-nailed device connections is that configuration is simplified, since it is not required that each non-nailed device be individually configured.

The host cannot make an outbound call to a non-nailed device.

Nailed Devices

A nailed device is one with a permanently assigned ldev. The assignment is configured on the MPE/iX host system. Nailed devices can be accessed programmatically through their ldev number. There is an ldev-to-25-address mapping. The host can support both inbound and outbound calls.

Configuration of Nailed Versus Non-Nailed Devices

Following are some points to remember when configuring nailed and non-nailed PAD devices:

- Printer must be nailed.
- Terminals may be nailed or non-nailed.
- Programmatic access requires a nailed device.
- Logon access may be either nailed or non-nailed.

Saving DTS Parameters

Make a list of the following DTS parameters configured n the host that must also be entered into the OpenView DTC Manager.

- Local Node Name.
- PAD Device Name.
- PAD Device Type.
- DTC Node Name.
- DTC Card Number.

Configuring the DTC

If you are using PC-based network management, configure the DTC by using the OpenView DTC Manager at your OpenView Windows Workstation. For full details, see *Using the OpenView DTC Manager*.

If you are using host-based network management, configure the DTC using NMMGR. For full details, see *Configuring and Managing Host-Based X.25 Links*.

D PCI 10/100Base-TX/3000 Quick Installation

The PCI 10/100Base-TX adapter card (A5230A) for the HP e3000 supports 10Mbits/s and 100Mbits/s Fast Ethernet operation as well as full and half-duplex modes. Ensure that the speed, duplex, and autonegotiation settings of the associated data hub or switch match the settings on this card (as configured in the network configuration file, NMCONFIG.PUB.SYS). Refer to the sections on “Notes on Manual Speed and Duplex Mode Configuration” and “Notes on Autonegotiation and Autosensing” in this appendix for background information on determining these settings, if needed. For a detailed description of using NMMGR to configure the 10/100Base-TX link in your NMCONFIG file, see the *NS 3000/iX NMMGR Screens Reference Manual*.

1. Verify the PCI 10/100Base-TX software is present in the installed version of MPE/iX (must be 7.0 or later).
   - Make sure MPE/iX 7.0 has been successfully installed on the system. The PCI 10/100Base-TX software license is included with MPE/iX 7.0. No additional software installation is required.
   - Run the `NMMAINT,78` command and verify complete version information is displayed for the PCI 100Base-TX link software (subsystem 78).

     Sample output:

```
:nmmaint,78

NMS Maintenance Utility  32098-20014 B.00.10  (C) Hewlett Packard Co.
1984


WED, DEC  6, 2000, 11:12 AM

Datacom products build version: N.73.01


Subsystem version IDs:

Subsystem Number : 78

PCI 100Base-T Fast Ethernet driver             module versions:


NL procedure:    PCI_100BT_NL_VERS          Version:  A0070072

XL procedure:    PCI_100BT_XL_VERS          Version:  A0070072

Catalog file:    NMCAT78.NET.SYS            Version:  A0070072

NL procedure:    LNK_NL_VERS                Version:  A0070004

NL procedure:    WANDMPSURRVERS             Version:  A0070000


PCI 100Base-T Fast Ethernet driver -------   overall version = A.00.70
```

2. Prepare system for hardware installation and access the system card bay:
   - Login with appropriate system management capabilities and prepare system for shutdown (e.g., terminate any active jobs or sessions, etc.)
   - Issue a **<ctrl-a>** shutdown. Make sure the system is halted before continuing.
   - When the system has shutdown completely, power off the system by pressing the system off button. Unplug the system.
   - Open the system to gain access to the PCI backplane, if applicable.
   - Select an empty PCI slot and remove the slot cover (if present).
3. Install the PCI 10/100Base-TX card:
   - Observe the antistatic precautions.
   - Record the serial number from the card, if present.
   - Grasp the card by its edges or faceplate with both hands, insert the card into the slot, and press the card firmly into place.
   - Secure the card and retaining screws (if present). Reassemble the system.
4. Attach the system to the network:
   - Attach the 8-pin (RJ-45) plug on your twisted-pair LAN cable into the RJ-45 connector on the card. The same RJ-45 connector is used for either 10 or 100Mbit/s operation.
   - Attach the free end of the cable to any unused port on the appropriate hub or switch (or into a wall jack that is connected to a hub or switch). Connect power to system. Set the hub or switch speed and duplex mode. The PCI 10/100Base-TX card operates in either full-duplex or half-duplex mode.
   - Power up the system.
   - Bring up the MPE/iX operating system.
5. Configure the link using NMMGR:
   - Run NMMGR and open the network configuration file (e.g., NMCONFIG.PUB.SYS).
   - Using “Guided Configuration”, configure or update the LAN Configuration. Change an existing, or add a new Network Interface (NI) so that the NI has a link Type of BT100, Enter the Physical path of the LANIC so that it references the path of the newly installed 10/100Base-T card.

- On the 100Base-T “link configuration” screen, fill in the appropriate autonegotiation, speed, and duplex settings. (For more detailed information on the various screens, see the *NS 3000/iX NMMGR Screens Reference Manual*.
- Perform configuration verification and exit NMMGR.

6. Verify the installation:

   - Verify that the link starts successfully by starting a network subsystem (e.g., `NETCONTROL START; NET=LAN1`) that uses the newly configured link.
   - Check console messages to verify that the link connected successfully. The link status can also be checked via the `LINKCONTROL` command. The following is a sample output for a successfully connected link:

```
:linkcontrol tslink;status=L

Linkname: LANLINK    Linktype: PCI 100BT        Linkstate: CONNECTED
```

   where “`LANLINK`” is the link name as configured in NMCONFIG on the “link configuration” data screen.

   - Verify that the card’s Link LED is on. Note that the LED cannot light unless the link software is also started.
   - Verify connectivity with a remote system, e.g., by issuing a “ping” command via the NETTOOL or PING utilities, or by establishing a remote VT session (after issuing an `NSCONTROL START`).

   If the link could not be brought up and the remote connection successfully verified, refer to the section on “Quick Troubleshooting Tips”.

Notes on Manual Speed and Duplex Mode Configuration

Because this PCI 10/100Base-TX LAN card supports autonegotiation, you should not normally need to manually set the duplex mode. Sometimes you may need to manually set the duplex mode of the card — for example, if the switch is operating at full duplex but does not autonegotiate.

Full-duplex mode is most commonly found in switches rather than hubs. It may be found in either 10 Mbit/s or 100Mbit/s switch devices. Full-duplex mode may provide a throughput advantage under some circumstances, but the degree of the advantage is application-dependent.

The PCI 10/100Base-TX card support both half- and full-duplex operation.

Ensure that the speed, duplex mode, and autonegotiation of the associated switch are configured the same as in the NMMGR configuration for the PCI 10/100Base-TX card. If the switch supports autonegotiation on the ports connected to the cards, this should be enabled as explained in “Notes on Autonegotiation and Autosensing.”

To manually set the duplex mode of the PCI card, refer to the link configuration screen in the active NMCONFIG network configuration file, using NMMGR to access the configuration data and make changes.

Notes on Autonegotiation and Autosensing

The PCI 10/100Base-TX/3000 product provides the means for interfacing various types of HP e3000 systems to either a 10Base-T or 100Base-TX network. 100Base-TX is a subset of 100Base-T networking defined by the IEEE 802.3u-1995 standard. 100Base-TX provides 100 Mbits/s data transmission over category 5 unshielded twisted-pair (UTP) cable for which two pairs of wires in the cable are used — one wire pair for receiving data, and one wire pair for transmitting data. The same card port that supports 100Base-TX operation can also support 10Base-T operation.

Autonegotiation is a mechanism defined in the IEEE 802.3u specification whereby devices sharing a link segment can exchange information while the link is being established and automatically configure themselves to operate at the most efficient mode shared between them.

Autonegotiation is like a rotary switch that automatically switches to the correct technology such as 10Base-T or 100Base-TX or between half- and full-duplex modes. Once the most efficient common mode is determined, autonegotiation passes control of the link to the appropriate technology, sets the appropriate duplex mode, and then becomes transparent until the link is broken.

The following is the IEEE 802.3u-defined autonegotiation hierarchy for resolving multiple common abilities for a 10/100Base-TX card:

- 100Base-TX full-duplex (most efficient)
- 100Base-TX half-duplex
- 10Base-T full-duplex
- 10Base-T half-duplex (least efficient)

For example, if both devices on the link support 10Base-T (half-duplex) and 100Base-TX (half-duplex), autonegotiation at both ends will select 100Base-TX (half-duplex) instead of 10Base-T (half-duplex).

Many 100Base-TX devices on the market today such as hubs and switches do not support autonegotiation. Either the speed and duplex mode of the device are fixed (as is usually the case with hubs), or they are often manually configured at the desired speed and duplex (as is often the case for switches). However, switches that support autonegotiation are becoming more commonplace

If the PCI 10/100Base-TX/3000 card is connected to a device, such as a switch, that is autonegotiating, the PCI card will autonegotiate with the device to mutually determine the highest possible speed and duplex settings between them.

If the PCI 10/100Base-TX/3000 card is connected to a device that does not support autonegotiation or a device that has autonegotiation disabled, the PCI card will autosense the speed of the link and set itself accordingly. *The duplex mode of the card will be set to half-duplex in this case.* If you want the card to operate in full-duplex mode, you must set it using the method described in “Notes on Manual Speed and Duplex Mode Configuration” in this document.

The PCI 10/100Base-TX card will sense when the connection between itself and a hub or switch on the other end of a link has been broken. If a connection is made to another (or the same) device and autonegotiation is enabled, the autonegotiation and autosensing process will be done again automatically. Autonegotiation and autosensing are also done whenever the interface is reset.

Quick Troubleshooting Tips

Problem: Incomplete version information displayed when `:NMMAINT,78` command is issued.

This indicates that the MPE/iX 7.0 software installation or update has not completed successfully. Consult your HP software support representative.

Problem: When an attempt is made to bring up the link (e.g., via a `:NETCONTROL START` command for a LAN using that link), it does not connect successfully. Connection failure messages are logged to the console or a `:LINKCONTROL linkname;STATUS=L` command shows the link as “DISCONNECTED”.

This often suggests an incompatibility between the card’s speed and duplex settings and the switch or hub settings. Make sure to review the settings for autonegotiation, speed and duplex in the link configuration data and make sure they are consistent with what the hub or switch expects and supports. Bring the LAN down (`:NETCONTROL STOP` or DTCCNTRL option 4) and back up again, to cause software to read the new configuration. If you still cannot connect successfully, make sure all the cables are securely connected between the card and the hub/switch and that the card is properly seated. If that fails, consult your HP support representative.

Index

X